Universidad Miguel Hernández de Elche

Departamento de Ciencias de Materiales, Óptica y Tecnología Electrónica

Técnicas de Reputación para Redes de Comunicaciones Inalámbricas Multi-Salto

Francisco Alberto Rodríguez Mayol

Director: Javier Gozálvez Sempere

Tesis para el grado de Doctor

Fecha: Julio 2013

UNIVERSITAS
Miguel
Hernández

Dª Mª JULIA ARIAS RODRÍGUEZ, Directora del Departamento de Ciencia de Materiales, Óptica y Tecnología Electrónica de la Universidad Miguel Hernández
de Elche,

INFORMA

favorablemente que la Tesis titulada "Técnicas de Reputación para Redes de Comunicaciones Inalámbricas Multi-Salto" de la que es autor el doctorando Francisco Alberto Rodríguez Mayol, y dirigida por el Dr. Javier Gozalvez Sempere, tiene la conformidad de este departamento para que sea depositada y presentada para su exposición pública, ya que cumple los requisitos en cuanto a forma y contenido.

Para que conste, en cumplimiento de la legislación vigente, firma la presente en Elche, a de de 2013.

Fdo. Dª Mª Julia Arias Rodríguez
Directora del Departamento de Ciencia de Materiales, Óptica y Tecnología Electrónica

JAVIER GOZÁLVEZ SEMPERE, Doctor Ingeniero, y profesor de la Universidad Miguel Hernández de Elche,

CERTIFICA

que la Tesis titulada "Técnicas de Reputación para Redes de Comunicaciones Inalámbricas Multi-Salto" de la que es autor el doctorando Francisco Alberto Rodríguez Mayol ha sido realizada bajo su dirección.

Considerando que se trata de un trabajo original de investigación que reúne los requisitos establecidos en la legislación vigente, autoriza su presentación. Y para que así conste, firma el presente certificado,

Elche, de de 2013

Fdo. Javier Gozálvez Sempere

Este trabajo fue financiado en parte por la Generalitat Valenciana a través de la Beca para Formación de Personal Investigador de Carácter Predoctoral BFPI/2007/269 y el proyecto ACOMP/2010/111, el Ministerio de Ciencia e Innovación del Gobierno de España y fondos FEDER a través del proyecto TEC2008-06728, el Ministerio de Industria, Turismo y Comercio del Gobierno de España a través del proyecto TSI-020400-2008-113 (CELTIC proposal CP5-013) y el Ministerio de Economía y Competitividad del Gobierno de España y fondos FEDER (TEC2011-26109).

UNIVERSITAS
Miguel
Hernández

Resumen

En las redes MANET, las funciones de establecimiento y mantenimiento de la red deben ser realizadas por los propios nodos que la componen de manera distribuida. Esta característica les otorga una gran versatilidad y adaptabilidad, pero al mismo tiempo exige que se preste una especial atención a la seguridad de la red, para garantizar su correcto funcionamiento. Entre las funciones que deben realizar los nodos que forman parte de una red MANET están el enrutamiento y la retransmisión de los paquetes. Estas funciones permiten que paquetes generados en un cierto nodo origen puedan ser encaminados y retransmitidos por distintos nodos retransmisores hasta llegar al nodo destino a través del medio inalámbrico, aunque origen y destino no se encuentren dentro del rango de transmisión directo. Estos procesos exigen la cooperación de los nodos que componen la red, que a cambio pueden disfrutar de las ventajas de su utilización en su propio beneficio. Sin esta cooperación, la conectividad de la red y su propia existencia se pueden ver seriamente comprometidas. La cooperación de los nodos en este tipo de redes debe ser incentivada para evitar que algunos nodos, denominados egoístas, utilicen la red sin prestar a cambio sus propios recursos de comunicación para su mantenimiento. En las técnicas de incentivo a cooperación basadas en reputación, cada nodo utiliza distintas herramientas para detectar a aquellos nodos que no cooperan adecuadamente en la retransmisión de los paquetes de datos. Su objetivo es evitar que los nodos egoístas participen como nodos retransmisores (ya que no son fiables y pueden descartar los paquetes en vez de retransmitirlos) o como orígenes o destino de datos (para incentivarlos a cooperar si quieren beneficiarse de la utilización de la red). En este contexto, la presente tesis se centra en el diseño y evaluación de técnicas de incentivo a la cooperación basadas en reputación capaces de detectar y aislar convenientemente a los nodos egoístas en redes MANET. En primer lugar se establecen y analizan las condiciones y los procedimientos apropiados para la evaluación correcta de las técnicas de reputación en una red MANET con presencia de nodos egoístas. Se demuestra que en trabajos anteriores no se había estudiado la importancia de la utilización de modelos de canal realistas para la evaluación del rendimiento de las técnicas de reputación. Tras el dimensionamiento de las condiciones de simulación, se aprecia un incremento notable del número de ocasiones en que las técnicas acusan incorrectamente a nodos cooperativos de estar comportándose egoístamente. Esto está motivado por la imprecisión del proceso de observación del comportamiento de los nodos, provocada por errores de transmisión radio y colisiones de paquetes. El efecto final de todo ello es que se reduce la conectividad de la red, debido a

que el aislamiento al que se somete a los nodos acusados incorrectamente provoca una reducción del número de rutas seguras. En este contexto, se proponen y analizan tres mecanismos que, mediante diferentes enfoques, tratan reducir el número de acusaciones incorrectas de las técnicas de reputación y paralelamente, aumentar el número de rutas seguras disponibles y la conectividad de la red. Por otro lado, se estudia el comportamiento de ciertos nodos egoístas que no descartan todos los paquetes que deben retransmitir, sino únicamente una fracción aleatoria de ellos. Este comportamiento hace más difícil su detección, que exhibe un compromiso entre la rapidez de detección y el error cometido al acusar a nodos cooperativos o no detectar a nodos egoístas. Se proponen y analizan técnicas de detección exponenciales que mejoran este compromiso frente a las tradicionales técnicas bayesianas. Además, en la última parte de la tesis, se propone aprovechar el uso de la infraestructura de red celular, en el marco de las redes de comunicaciones multi-salto celulares, para mejorar las características de seguridad de las redes MANET convencionales. En este contexto, se diseñan y evalúan técnicas de reputación que logran alcanzar los objetivos de rendimiento planteados inicialmente: aislamiento efectivo de los nodos con un comportamiento egoísta y salvaguarda y aumento de la conectividad de los nodos cooperativos.

UNIVERSITAS
Miguel
Hernández

UNIVERSITAS
Miguel
Hernández

Agradecimientos

Este trabajo no habría sido posible sin el apoyo y la ayuda de mi director Javier Gozálvez Sempere. Sin su trabajo de supervisión, orientación, inspiración, corrección, motivación y comprensión en los malos momentos, este trabajo nunca habría podido finalizarse. Me siento en deuda por su dedicación a lo largo de estos años.

También agradezco la ayuda de mis compañeros en el laboratorio UWICORE, en el cual fue realizada esta tesis. Siempre he tenido su apoyo, su colaboración, su ayuda, su compañerismo, sus palabras de aliento, las bromas, su preocupación desinteresada, que hicieron que el trabajo se desarrollara en un ambiente a la vez profesional y serio, y entre amigos, y por tanto, mucho más llevadero.

También valoro la ayuda recibida por parte de los compañeros del departamento de Ingeniería de Comunicaciones de la Universidad Miguel Hernández, y el de Ciencias de Materiales, Óptica y Tecnología Electrónica, así como todo el personal que trabaja en los edificios Quórum V, Torrepinet, Altabix y Rectorado, con los que he coincidido y otros profesionales y trabajadores de la universidad que han facilitado mi trabajo a lo largo de estos años.

También quiero agradecer el cariño y el apoyo de esas otras personas tan necesarias en la vida, los amigos y colegas, los de la universidad, los del instituto, los de remo UA y todos los demás, que también han hecho que esta tesis haya sido posible, gracias a su apoyo y a la distracción necesaria en los momentos de esparcimiento que me permitieron poder retomar el trabajo con empeño renovado.

Pero sin duda mi mayor agradecimiento va para las personas más cercanas a mí, los que forman parte de mi familia, los de verdad y aquellos a los que también considero como tal aunque no lo sean. Sin su apoyo en todas las dificultades con las que nos hemos encontrado en estos años, no habría podido seguir adelante. Su cariño es la principal motivación para hacer las cosas bien. A la persona que más ilusión le hace que acabe esta tesis, mi padre, luchador incansable, se la dedico, a mi hermana, imprescindible para que las cosas sigan adelante, y a mi madre, una de las personas más extraordinarias que conocí.

Contenidos

Publicaciones ..... **xix**

Acrónimos ..... **xxi**

Figuras ..... **xxix**

Tablas ..... **xxxv**

1 Introducción **1**

2 Técnicas de incentivo a la cooperación **9**

2.1 Cooperación en redes MANET 10

2.1.1 Tipos de comportamiento no cooperativo 10

2.1.2 Efectos del comportamiento egoísta 14

2.2 Técnicas de incentivo a la cooperación 14

2.2.1 Técnicas basadas en crédito 15

2.2.2 Técnicas basadas en teoría de juegos 20

2.2.3 Otras técnicas 25

2.3 Técnicas basadas en reputación 27

2.3.1 Revisión de técnicas de reputación 29

2.4 Dimensionamiento y viabilidad de técnicas basadas en reputación 35

2.5 Técnicas de detección 37

2.6 Técnicas de reputación con asistencia centralizada 40

2.7 Resumen 42

3 Redes inalámbricas **45**

3.1 Redes MANET 46

3.2 Capa PHY 802.11a 48

3.2.1 Subcapa PMD 49

3.2.2 Subcapa PLCP 51

3.3 Capa MAC 802.11a 53

3.3.1 Método de acceso DCF 53

3.3.2 Sincronización 54

3.3.3 Protocolo RTS/CTS 55

3.4 802.11s: comunicaciones *mesh* en redes multi-salto 57

3.5 Protocolo DYMO 58

3.6 Redes celulares 69

3.6.1 HSDPA 70

4 Entorno de evaluación 73
4.1 Simulador de comunicaciones ns-2 74
4.1.1 Descripción y funcionalidades 74
4.1.2 Arquitectura básica 75
4.1.3 Proceso de simulación en ns-2 77
4.2 Implementación de sistemas de comunicaciones inalámbricos en ns-2 78
4.2.1 Modelos de propagación 81
4.2.2 Capa PHY 802.11 en ns-2 85
4.2.3 Capa MAC 802.11 en ns-2 88
4.3 Escenarios y parámetros de configuración 90
4.3.1 Patrones de tráfico de usuario 90
4.3.2 Topología del escenario 91
4.3.3 Movilidad 92
4.3.4 Modelos de canal 93

5 Dimensionado y viabilidad de técnicas de reputación en redes MANET 95
5.1 Nodos no cooperativos en redes MANETs 96
5.2 Técnica de observación *watchdog* 99
5.3 Técnica de Marti 102
5.4 Técnica TEAM 105
5.5 Evaluación en condiciones realistas 107
5.5.1 Métricas de evaluación de rendimiento 107
5.5.2 Plataforma y escenarios de evaluación 110
5.5.3 Número de saltos por transmisión multi-salto 112
5.5.4 Capacidad de detección de nodos egoístas 116
5.5.5 Tasa de entrega y pérdidas de paquetes 119
5.6 Conclusiones 122

6 Nuevas propuestas de técnicas de reputación distribuidas 125
6.1 Reset Activity Mode 126
6.2 Warning Mode 128
6.3 Reset Failure Mode 130
6.4 Evaluación 132
6.4.1 Métricas de evaluación 132
6.4.2 Escenarios de simulación 134
6.4.3 Análisis comparativo 135
6.5 Conclusiones 149

7 Detección Bayesiana y exponencial 151
7.1 Técnicas de detección Bayesianas 152
7.1.1 Descripción y variantes 152
7.1.2 Análisis por cadenas de Markov 156

7.2 Técnica de vigilancia exponencial 161
7.3 Evaluación experimental 168
7.3.1 Métricas de evaluación 168
7.3.2 Escenarios de evaluación 169
7.3.3 Velocidad y precisión de detección 172
7.3.4 Sensibilidad al error de estimación de probabilidad de error 177
7.4 Conclusiones 180

8 Técnicas de reputación en redes multi-salto celular 183
8.1 Técnica BC (*Broadcast Category*) 185
8.2 Técnica SC (*Selfishness Check*) 191
8.3 Evaluación experimental 197
8.3.1 Métricas de rendimiento 198
8.3.2 Escenarios de evaluación 200
8.3.3 Técnicas de referencia 201
8.3.4 Técnicas centralizadas en redes MCN 203
8.3.5 Señalización de técnicas centralizadas 211
8.3.6 Capacidad de detección 215
8.3.7 Capacidad de reacción 218
8.4 Conclusiones 220

9 Conclusiones 223
9.1 Dimensionamiento y viabilidad de sistemas de reputación en redes MANET 224
9.2 Técnicas de reputación distribuidas 225
9.3 Detección Bayesiana y exponencial 227
9.4 Técnicas de reputación en redes multi-salto celular 228
9.5 Líneas futuras de investigación 230

A-I Interfaz radio celular en la herramienta ns-2 235

A-II Estimación del parámetro de probabilidad de error p_e 243

Bibliografía 251

UNIVERSITAS
Miguel
Hernández

Publicaciones

Hasta la fecha, el trabajo realizado en la presente tesis ha generado las siguientes publicaciones:

Publicaciones:

A. Rodriguez-Mayol y J. Gozalvez, "Detection mechanism for reputation-based selfishness prevention in MANETs", *Transactions on Emerging Telecommunications Technologies ETT*, 20 Junio 2012. doi: 10.1002/ett.2545

A. Rodriguez-Mayol y J. Gozalvez, "Reputation Based Selfishness Prevention Techniques for Mobile Ad-hoc Networks", *Telecommunications System Journal*. (aceptado para su publicación).

Congresos:

A. Rodriguez-Mayol y J. Gozalvez, "Improving Selfishness Detection in Reputation Protocols for Cooperative Mobile Ad-hoc Networks", *Libro de Actas del 21st IEEE Personal, Indoor and Mobile Radio Communications Symposium (PIMRC'10)*, 26-29 Septiembre 2010, Estambul (Turquía).

A. Rodriguez-Mayol y J. Gozalvez, "On the Implementation Feasibility of Reputation Techniques for Cooperative Mobile Ad-hoc Networks", *Libro de Actas del 16th European Wireless Conference (EW2010)*, 12-15 Abril 2010, Lucca (Italia).

Alberto Rodriguez-Mayol y J. Gozalvez, "Mecanismo de Detección de Egoísmo para Sistemas de Reputación en MANETs", *Libro de Actas del XXVII Simpósium Nacional de la Unión Científica Internacional de Radio (URSI),* 12-14 Septiembre 2012*,* Elche.

A. Rodriguez-Mayol y J. Gozalvez, "Prevención de Egoísmo Basada en Verosimilitud en Redes MANET", *Libro de Actas de las X Jornadas de Ingeniería Telemática (Jitel 2011)*, 28-30 Septiembre 2011, Santander.

A. Rodriguez-Mayol y J. Gozalvez, "Sistemas Avanzados de Reputación para Redes Móviles Ad-hoc Cooperativas", *Libro de Actas de las IX Jornadas de Ingeniería Telemática (Jitel 2010)*, 29 Septiembre - 1 Octubre 2010, Valladolid.

A. Rodriguez-Mayol y J. Gozalvez, "Implementación de Técnicas de Reputación en Redes MANET Cooperativas", *Libro de Actas de las XIX Jornadas de Telecom I+D*, 24-26 Noviembre 2009, Madrid.

Acrónimos

16-QAM	16 – Quadrature Amplitude Modulation
3GPP	3rd Generation Partnership Project
ACK	ACKnowledgment
ANSI	American National Standards Institute
AODV	Ad-hoc On-demand Distance Vector routing protocol
AODVv2	DYnamic MANET On-demand routing protocol
AOMDV	Ad-hoc On-demand Multipath Distance Vector routing protocol
ARIB	Alliance of Radio Industries and Business
ARP	Address Resolution Protocol
BC	Broadcast Category
BER	Bit Error Rate
BPSK	Binary Phase Shift Keying
BTS	Base Transceiver Station
CAHN	Cellular Assisted Heterogeneous Networking
CBR	Constant Bit Rate
CCS	Credit Clearance Service
CDF	Cumulative Distribution Function
CEPT	European Conference of Postal and Telecommunications
CM	Central Manager
CN	Cellular Network
CONFIDANT	Cooperation Of Nodes: Fairness In Dynamic Ad-hoc NeTworks

CORE	COllaborative REputation system
CQI	Channel Qualitity Indicator
CRC	Cyclic Redundancy Check
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
CTS	Clear To Send
CW	Contention Window
DCF	Distributed Coordination Function
DIFS	Distributed InterFrame Space
DoS	Denial of Service
DPCCH	Deditated Physical Control Channel
DPDCH	Deditated Physical Data Channel
DPSK	Differential Phase Shift Keying
DSDV	Destination-Sequenced Distance Vector routing protocol
DSN	Destination Sequence Number
DSR	Dynamic Source Routing protocol
DSSS	Direct-Sequence Spread Spectrum
DYMO[1]	DYnamic MANET On-demand routing protocol
EIFS	Extended InterFrame Space
EIRP	Equivalent Isotropically Radiated Power
ETSI	European Telecommunications Standards Institute
EU	European Union
FCC	Federal Communications Commision
FER	Frame Error Ratio
FHSS	Frequency-Hopping Spread Spectrum
FTP	File Transport Protocol
GAF	Geographic Adaptative Fidelity
GPRS	General Packet Radio System

[1] DYMO pasó a llamarse AODVv2 a partir de la versión 22 del correspondiente borrador de Internet de la IETF [25].

GSM	Global System for Mobile Communications
GTFT	Generous Tit-For-Tat
HARQ	Hybrid Automatic Repeat ReQuest
HDLC	High-Level Data Link Control
HSDPA	High-Speed Download Packet Acces
HS-DPCCH	High-Speed Dedicated Physical Control Channel
HS-DSCH	High-Speed Downlink Shared Channel
HSPA	High-Speed Packet Access
HS-PDSCH	High-Speed Physical Downlink Shared Channel
HS-SCCH	High-Speed Shared Control Channel
HSUPA	High-Speed Uplink Packet Acces
HSUPA	High-Speed Uplink Packet Access
HTML	HyperText Markup Language
HTTP	HyperText Transfer Protocol
HWMP	Hybrid Wireless Mesh Protocol
IBSS	Independent Basic Service Set
IEEE	Institute of Electrical And Electronics Engineers
IETF	Internet Engineering Task Force
IF_Range	Interference Range
IMEP	Internet MANET Encapsulation Protocol
IP	Internet Protocol
ISI	Inter-Symbol Interference
ISO	International Organization for Standardization
ITU	International Telecommunications Union
KPI	Key Performance Indicator
LA	Link Adaptation
LDP	Label Distribution Protocol
LLC	Logical Link Control
LOS	Line Of Sight

LUT	Look-Up Table
MAC	Medium Access Control
MANET	Mobile Ad-hoc NETwork
MCM	Multi-Carrier Modulation
MCN	Multi-hop Cellular Network
MDA	Mesh Deterministic Access
m-GTFT	multiple-GTFT
MIC	Ministry of Internal Affairs and Communications
MIMO	Multiple Input Multiple Output
MP	MultiPath fading
MPDU	MAC Protocol Data Unit
MPLS	Multiprotocol Label Switching
NAM	Numbers of Alleeged Manipulation
NAV	Network Allocation Vector
NLOS	Non-Line of Sight
NMT	Nordic Mobile Telephone
OFDM	Orthogonal Frequency Division Multiplexing
OLSR	Omptimized Link State Routing
OSI	Open System Interconnection
P2P	Peer to Peer
PCF	Point Coordination Function
PCS_Range	Physical Carrier Sensing Range
PD	Perfect Detection
PDA	Portable Device Assistant
PER	Packet Error Rate
PGM	Pragmatic General Multicast
PHY	Physical layer
PIFA	Protocol-Independent Fairness Algorithm
PL	Path Loss

PLCP	Physical Layer Convergence Procedure
PLM	Packet-pair receiver-driven cumulative Layer Multicast
PMD	Physical Medium Dependent
PPDU	PLCP Protocol Data Unit
PPM	Packet Purse Model
Pr	Potencia de recepción
PSDU	Physical Service Data Unit
Pt	Potencia de transmisión
PTM	Packet Trade Model
QAM	Quadrature Amplitude Modulation
QoS	Quality of Service
QPSK	Quadrature Phase-Shift Keying
RAM	Reset Activity Mode
RED	Random Early Detection
REM	Random Exponential Marking
RFC	Request For Comments
RFM	Reset Failure Mode
RIO	RED with In/Out
RLC	Radio Link Control
RLM	Receiver-driven Layered Multicast
RREP	Route REPly
RREQ	Route REQuest
RSSI	Received Signal Strength Indicator
RTS	Request To Send
RTT	Round-Trip Time
SC	Selfishness Check
SECM	SECurity Message
SH	SHadowing
SIFS	Short InterFrame Space

SINR	Signal to Interference and Noise Ratio
SIR	Signal to Interference Ratio
SMT	Secure Message Transmission
SPRITE	Simple, cheat-PRoof credIT-based system
SRM	Scalable Reliable Multicast
SRR	Semantic Packet Queue
TACS	Total Access Communications System
TCP	Transport Control Protocol
TEAM	Trust Enhanced security Architecture for Mobile ad-hoc networks
TORA	Temporally Ordered Routing Protocol
TPDU	Transport Protocol Data Unit
TTI	Transmission Time Interval
TX_Range	Transmission Range
UDP	User Datagram Protocol
SCTP	Stream Control Transmission Protocol
XCP	eXplicit Control Protocol
TFRC	TCP Friendly Rate Control
RAP	Route Access Protocol
RTP	Real time Transport Protocol
UMTS	Universal Mobile Telecommunications System
U-NII	Unlicensed – National Information Infrastructure
VANET	Vehicular Ad-hoc Networks
VBR	Variable Bit Rate
VQ	Virtual Queuing
WFQ	Weighted Fair Queuing
WiFi	Wireless-Fidelity
WLAN	Wireless Local Area Network
WM	Warning Mode

WPAN	Wireless Personal Area Network
WSN	Wireless Sensor Networks

UNIVERSITAS
Miguel
Hernández

Figuras

Figura 1-1. Diagrama de red MANET. 1
Figura 1-2. Diagrama de red MCN. 2
Figura 2-1. Diagrama general de técnicas de reputación. 38
Figura 3-1. Arquitectura de capas en 802.11. 49
Figura 3-2. Subportadoras OFDM consecutivas. 50
Figura 3-3. Mapeado de trama desde la capa MAC a la capa PLCP [3]. 52
Figura 3-4. Diagrama de la arquitectura de la capa MAC 802.11. 53
Figura 3-5. Funcionamiento de método de acceso DCF. 54
Figura 3-6. Zona de colisión por terminal escondido. 56
Figura 3-7. Descubrimiento de rutas, paso 1: origen comienza búsqueda de ruta. 59
Figura 3-8. Descubrimiento de rutas, paso 2: nodos adyacentes difunden RREQ. 62
Figura 3-9. Descubrimiento de rutas, paso 3: difusión de RREQ. 64
Figura 3-10. Descubrimiento de rutas, paso 4: la petición de ruta llega al destino. 65
Figura 3-11. Descubrimiento de rutas, paso 5: encaminamiento del RREP en la ruta inversa. 66
Figura 3-12. Ruptura de un enlace en la ruta. 67
Figura 4-1. Módulos de Nodo móvil, Canal inalámbrico y Antenas y propagación en ns-2. 78
Figura 4-2. Funcionamiento del canal radio en ns-2. 78
Figura 4-3. Diagrama de bloques de un nodo móvil asociado a un canal radio. 80
Figura 4-4. Condiciones LOS y NLOS en entorno urbano. 83
Figura 4-5. Efectos de la propagación radio en condiciones NLOS. 84
Figura 4-6. Configuración de la interfaz física de los nodos móviles de ns-2 86
Figura 4-7. Esquema empleado por ns-2 para determinar la recepción de un paquete. 86
Figura 4-8. Cálculo de interferencia mejorado. 87
Figura 4-9. Configuración de los parámetros MAC para IEEE 802.11a en ns-2. 88
Figura 4-10. Representación de la posición inicial de los nodos en el escenario Manhattan. 93
Figura 5-1. Funcionamiento del método de observación *watchdog*. 99
Figura 5-2. Distribución del tiempo de observación de la retransmisión. 101
Figura 5-3. Parámetros y factores que influyen en la conectividad de la red en presencia de nodos egoístas. 108

Figura 5-4. Distribución de la probabilidad de escoger aleatoriamente una ruta con nodos egoístas 109
Figura 5-5. Transmisión mediante modelo de propagación de 2 Rayos y LOS-NLOS. 113
Figura 5-6. PDR de distintos protocolos considerando el modelo de propagación de 2 Rayos.....120
Figura 5-7. PDR de distintos protocolos considerando el modelo de propagación Realista. 120
Figura 5-8. PDR de distintos protocolos considerando el modelo de propagación Realista y una carga de tráfico elevada. 121
Figura 5-9. PDR de la técnica TEAM considerando el modelo de propagación Realista y distintas condiciones del escenario. 121
Figura 6-1. Pseudocódigo de la técnica RAM. 127
Figura 6-2. Pseudocódigo de la técnica WM 130
Figura 6-3. Pseudocódigo de la técnica RFM 132
Figura 6-4. Porcentaje de paquetes perdidos sin ruta respecto a la técnica original de Marti. 138
Figura 6-5. Porcentaje de paquetes perdidos sin ruta respecto a la técnica original TEAM. 138
Figura 6-6. PDR obtenido con las técnicas propuestas respecto a la técnica original de Marti. 139
Figura 6-7. PDR obtenido con las técnicas propuestas respecto a la técnica original TEAM. 139
Figura 6-8. Porcentaje de paquetes descartados por nodos egoístas respecto a la técnica original de Marti 141
Figura 6-9. Porcentaje de paquetes descartados por nodos egoístas respecto a la técnica original TEAM 141
Figura 6-10. Porcentaje de paquetes perdidos por caídas de enlace respecto la técnica de Marti. 142
Figura 6-11. Porcentaje de paquetes perdidos por caídas de enlace respecto a la técnica TEAM. 143
Figura 6-12. Porcentaje de paquetes descartados por origen no seguro respecto a la técnica TEAM. 143
Figura 6-13. PDR de las técnicas con Marti para distintos niveles de error de transmisión radio. 144
Figura 6-14. PDR de las técnicas con TEAM para distintos niveles de error de transmisión radio. 145
Figura 6-15. Paquetes perdidos sin ruta para distintos niveles de error de transmisión radio. 145
Figura 6-16. Paquetes descartados por egoístas para distintos niveles de error de transmisión radio. 145
Figura 6-17. PDR de las técnicas con Marti para distintas tasas de colisiones de paquetes. 146
Figura 6-18. PDR de las técnicas con TEAM para distintas tasas de colisiones de paquetes. 147
Figura 6-19. Paquetes perdidos sin ruta para distintas tasas de colisiones de paquetes. 147
Figura 6-20. Paquetes descartados por nodos egoístas para distintas tasas de colisiones de paquetes 147
Figura 6-21. Número de establecimientos de ruta incorrectos con las técnicas propuestas respecto a TEAM para diferentes tasas de colisiones de paquetes 148

Figura 6-22. Número de negaciones correctas de ruta con las técnicas propuestas respecto a TEAM para diferentes tasas de colisiones de paquetes 148
Figura 7-1. Muestras del proceso aleatorio de observación de las retransmisiones. 154
Figura 7-2. Diagrama del modelo de cadenas de Markov del proceso de detección. 156
Figura 7-3. *IA* e *INA* en función del umbral de acusación τ. La leyenda corresponde a diferentes valores de p_s. 160
Figura 7-4. *IA* e *INA* en función del mínimo número de observaciones *l*. La leyenda corresponde a diferentes valores de p_s 160
Figura 7-5. *IA* e *INA* en función de la probabilidad de error p_e. La leyenda corresponde a diferentes valores de p_s. 161
Figura 7-6. Función de distribución Binomial $F(k;n,p)$, aproximación basada en la desigualdad de Hoeffding y función exponencial propuesta F_e 163
Figura 7-7. Muestra aleatoria del proceso de observación de retransmisiones (a) y representación de la función métrica exponencial F_e con distintos promedios (b). 165
Figura 7-8. Representación y parámetros de las funciones exponencial y Bayesiana. 168
Figura 7-9. Distintas distribuciones de probabilidad del parámetro p_s 172
Figura 7-10. Tasa de acusaciones incorrectas en función del número máximo de observaciones. 174
Figura 7-11. Tasa de no acusaciones incorrectas en función del número máximo de observaciones. 174
Figura 7-12. Número de paquetes descartados por egoístas antes de su detección en función del número máximo de observaciones 175
Figura 7-13. Tasa de acusaciones incorrectas en función del error de observación p_e 176
Figura 7-14. Tasa de no acusaciones incorrectas en función del error de observación p_e. 177
Figura 7-15. Número de paquetes descartados por nodos egoístas antes de su detección δ en función del error de observación p_e 177
Figura 7-16. Tasa de acusaciones incorrectas *IA* en función de la desviación en la estimación del error de observación p_e 179
Figura 7-17. Tasa de no acusaciones incorrectas *INA* en función de la desviación en la estimación del error de observación p_e. 179
Figura 7-18. Número de paquetes descartados por nodos egoístas antes de su detección δ en función de la desviación en la estimación del error de observación p_e. 180
Figura 8-1. Detección local de nodo egoísta. 186
Figura 8-2. Aislamiento local de nodo egoísta. 187
Figura 8-3. Detección local y difusión de identidad de nodo egoísta. 188
Figura 8-4. Aislamiento global de nodo egoísta. 188
Figura 8-5. Pseudocódigo de la técnica BC. 191
Figura 8-6. Proceso de comprobación de técnica *Selfishness Check*. 192
Figura 8-7. Pseudocódigo de la técnica SC. 196

Figura 8-8. Pseudocódigo de la técnica BC+SC. 197
Figura 8-9. PDR de técnicas de referencia en escenario I. 203
Figura 8-10. PDR de técnicas de referencia en escenario II. 203
Figura 8-11. PDR de la técnica BIW y técnicas centralizadas BC y SC en escenario I. 205
Figura 8-12. PDR de la técnica BDF y técnicas centralizadas BC y SC en escenario I. 205
Figura 8-13. PDR de la técnica EIW y técnicas centralizadas BC y SC en escenario I. 205
Figura 8-14. PDR de la técnica EFW y técnicas centralizadas BC y SC en escenario I. 205
Figura 8-15. PDR de la técnica BIW y técnicas centralizadas BC y SC en escenario II. 207
Figura 8-16. PDR de la técnica BDF y técnicas centralizadas BC y SC en escenario II. 207
Figura 8-17. PDR de la técnica EIW y técnicas centralizadas BC y SC en escenario II. 207
Figura 8-18. PDR de la técnica EFW y técnicas centralizadas BC y SC en escenario II. 207
Figura 8-19. % paquetes sin ruta de la técnica BIW y técnicas centralizadas escenario I. 208
Figura 8-20. % paquetes sin ruta de la técnica EIW y técnicas centralizadas escenario I. 208
Figura 8-21. % paquetes sin ruta de la técnica BIW y técnicas centralizadas escenario II. 208
Figura 8-22. % paquetes sin ruta de la técnica EIW y técnicas centralizadas escenario II. 208
Figura 8-23. % paquetes descartados por nodos egoístas de la técnica BIW y técnicas centralizadas en escenario I. 210
Figura 8-24. % paquetes descartados por nodos egoístas de la técnica EIW y técnicas centralizadas en escenario I. 210
Figura 8-25. % paquetes descartados por nodos egoístas de la técnica BIW y técnicas centralizadas en escenario II. 210
Figura 8-26. % paquetes descartados por nodos egoístas de la técnica EIW y técnicas centralizadas en escenario II. 210
Figura 8-27. % paquetes descartados por caída de enlace de la técnica BIW y técnicas centralizadas en escenario I 211
Figura 8-28. % paquetes descartados por origen sospechoso de la técnica BIW y técnicas centralizadas en escenario I 211
Figura 8-29. Diagrama temporal de mensajes en el proceso BC. 212
Figura 8-30. Diagrama temporal de mensajes en el proceso BC+SC 213
Figura 8-31. % de nodos acusados de técnica BIW y técnicas centralizadas en escenario I 216
Figura 8-32. % de nodos acusados de técnica BIW y técnicas centralizadas en escenario II 216
Figura 8-33. % de nodos acusados de técnica EIW y técnicas centralizadas en escenario I 216
Figura 8-34. % de nodos acusados de técnica EIW y técnicas centralizadas en escenario II 216
Figura 8-35. Paquetes descartados antes de detección de técnica BIW y de técnicas centralizadas escenario I 218
Figura 8-36. Paquetes descartados antes de detección de técnica EIW y de técnicas centralizadas escenario I 218

Figura 8-37. Paquetes descartados por nodos egoístas en función del egoísmo del nodo origen, técnica BIW y centralizadas escenario I 219
Figura 8-38. Paquetes descartados por nodos egoístas en función del egoísmo del nodo origen, técnica EIW y centralizadas escenario I.....219
Figura 8-39. Número total acusaciones, técnica BIW y centralizadas, escenario I 219
Figura 8-40. Número total acusaciones, técnica EIW y centralizadas, escenario I 219
Figura A-1-1. Diagrama de nodos híbridos y nodos ad-hoc en una red MCN. 236
Figura A-I-2. CQI en función de la distancia de campaña de medidas 239
Figura A-I-3. Probabilidad de cumplimiento de requisito de calidad enlace radio. 240
Figura A-II-1. PDR de la técnica BIW con distintas configuraciones de p_e en escenario I.....246
Figura A-II-2. PDR de la técnica BDF con distintas configuraciones de p_e en escenario I.....246
Figura A-II-3. PDR de la técnica EIW con distintas configuraciones de p_e en escenario I.....246
Figura A-II-4. PDR de la técnica EFW con distintas configuraciones de p_e en escenario I. 246
Figura A-II-5. PDR de la técnica BIW con distintas configuraciones de p_e en escenario II. 247
Figura A-II-6. PDR de la técnica BDF con distintas configuraciones de p_e en escenario II. 247
Figura A-II-7. PDR de la técnica EIW con distintas configuraciones de p_e en escenario II.....247
Figura A-II-8. PDR de la técnica EFW con distintas configuraciones de p_e en escenario II.....247
Figura A-II-9. CDF de la estimación del parámetro p_e experimentado. 249

UNIVERSITAS
Miguel
Hernández

Tablas

Tabla 2-1. Tipos de comportamiento no cooperativo. 13
Tabla 2-2. Técnicas de incentivo a cooperación basadas en crédito. 18
Tabla 2-3. Trabajos y técnicas de incentivo a cooperación que emplean la teoría de juegos. 23
Tabla 2-4. Técnicas de incentivo a cooperación pertenecientes a otras categorías. 27
Tabla 2-5. Técnicas de incentivo a cooperación basadas en reputación. 33
Tabla 2-6. Valores de parámetros de simulación de técnicas de incentivo a cooperación. 36
Tabla 2-7. Técnicas de observación de comportamiento basadas en *watchdog*. 39
Tabla 2-8. Técnicas de incentivo a cooperación centralizadas basadas en reputación. 41
Tabla 3-1. Parámetros OFDM de IEEE 802.11a. 50
Tabla 3-2. Potencias máximas de transmisión. 51
Tabla 3-3: Tasas de transmisión posibles en IEEE 802.11a. 52
Tabla 3-4. Estructura de los mensajes de enrutamiento RREQ y RREP. 59
Tabla 3-5. Mensaje RREQ originado a partir del ejemplo en la Figura 3-7. 60
Tabla 3-6. Tabla de rutas del nodo *2* en la Figura 3-7. 62
Tabla 3-7. Mensaje RREQ reenviado por el nodo *2* a partir del ejemplo en la Figura 3-8. 62
Tabla 3-8. Tabla de rutas del nodo *4* en la Figura 3-8. 63
Tabla 3-9. Mensaje RREQ reenviado por el nodo *4* a partir del ejemplo en la Figura 3-9. 63
Tabla 3-10. Tabla de rutas del nodo *6* en la Figura 3-9. 64
Tabla 3-11. Tabla de rutas del nodo *8* en la Figura 3-10. 65
Tabla 3-12. Mensaje RREP generado por el nodo *8* a partir del ejemplo en la Figura 3-11. 65
Tabla 3-13. Tabla de rutas de los nodos *6*, *4* y *2* en la Figura 3-10. 66
Tabla 3-14. Valores por defecto de algunos de los temporizadores usados en DYMO. 68
Tabla 3-15. Comparativa de características de UMTS y HSDPA. 71
Tabla 4-1 Protocolos y modelos de tecnologías de comunicación en ns-2. 75
Tabla 4-2. Modelos de pérdidas básicas de propagación incluidos en ns-2. 82
Tabla 4-3. Valores típicos del exponente de *pathloss* del modelo de propagación *Shadowing*. 82
Tabla 4-4. Valores típicos de la desviación típica del desvanecimiento del modelo de propagación *Shadowing*. 82

Tabla 4-5. Valores promedio de los parámetros del modelo de tráfico web.....90
Tabla 4-6. Tiempo entre sesiones promedio del modelo de tráfico web. 91
Tabla 4-7. Número de nodos y dimensiones de los escenarios.....92
Tabla 5-1 Parámetros de configuración de la técnica de Marti. 103
Tabla 5-2 PDR de nodos egoístas y cooperativos. 104
Tabla 5-3 Parámetros de configuración del protocolo TEAM.....107
Tabla 5-4 Configuración de parámetros de simulación. 112
Tabla 5-5 Distancia total extremo a extremo [m]. 114
Tabla 5-6 Distancia de salto [m].....115
Tabla 5-7 Número de saltos promedio por ruta establecida y por paquete recibido. 116
Tabla 5-8 Parámetros de detección de Marti y TEAM en distintos escenarios. 117
Tabla 6-1 Configuración de parámetros de simulación. 135
Tabla 6-2 Mejora obtenida con las técnicas propuestas respecto a la técnica de Marti original....137
Tabla 6-3 Mejora obtenida con las técnicas propuestas respecto a la técnica TEAM original. 137
Tabla 7-1. Requisitos de la función F_e. 162
Tabla 7-2. Error relativo máximo [%]. 170
Tabla 7-3. Valores de τ para rendimiento promedio optimizado. 173
Tabla 7-4. Valores de l para rendimiento promedio optimizado. 173
Tabla 8-1 Configuración de parámetros de simulación. 201
Tabla 8-2. Sobrecarga por señalización de mensajes de procesos SC 213
Tabla 8-3. Sobrecarga por señalización de mensajes de procesos BC.....214
Tabla A-I-1 Mapeo entre el valor de CQI y parámetros de transmisión de LA.....238
Tabla A-II-1. Valores seleccionados de p_e, τ y l empleados en las simulaciones del capítulo 8 ...248

1

Introducción

Las redes móviles *ad-hoc* (MANET *Mobile Ad-hoc NETworks*) se caracterizan por no utilizar una infraestructura fija, pudiendo variar en ellas el número de nodos, su topología, y también la distribución jerárquica de las funciones de establecimiento y mantenimiento de la red (Figura 1-1). Por consiguiente, estas funciones deben ser realizadas por los propios nodos que la componen, de manera distribuida, para poder adaptarse a las circunstancias variables del escenario de despliegue. Entre las ventajas que ofrecen las redes MANET cabe citar la versatilidad, la adaptabilidad a escenarios variables, la posibilidad de operar sin infraestructura fija con su consecuente ahorro económico, y la facilidad de configuración y establecimiento de la red. Estas características las hacen útiles en aplicaciones actuales tales como despliegues en escenarios de emergencia, redes de sensores, redes vehiculares, redes oportunistas, etc.

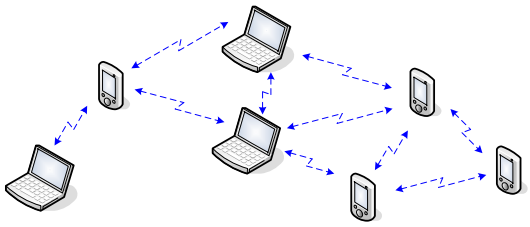


Figura 1-1. Diagrama de red MANET.

Relacionadas con las anteriores, las redes multi-salto celulares o MCN (*Multi-hop Cellular Networks*) combinan las características de las redes MANET y de las redes móviles celulares (Figura 1-2). Como en las redes celulares, los usuarios pueden conectarse con la red troncal en toda la zona geográfica cubierta por las estaciones base celulares tradicionales. Sin embargo, en las redes multi-salto celulares, no se requiere la existencia de un enlace de comunicación entre la estación móvil y la estación base. De hecho, la comunicación entre la estación móvil y la estación base es, en general, transmitida por un número de otras estaciones móviles, de manera similar a como ocurre en una MANET. Una de las principales ventajas de las redes multi-salto celulares es que aprovechan las características complementarias de las redes celulares y de las redes MANET. Esta sinergia se utilizará para diseñar algunas de las técnicas propuestas en este trabajo de tesis. Los primeros capítulos tratarán exclusivamente sobre redes MANET, mientras que el último explotará la potencialidad de las redes MCN.

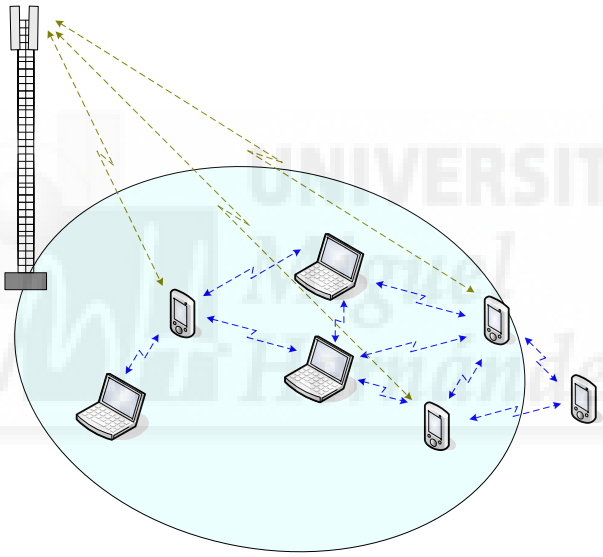


Figura 1-2. Diagrama de red MCN.

Entre las funciones que deben realizar los nodos que forman parte de una red MANET están el enrutamiento y la retransmisión de los paquetes. Estas funciones permiten que paquetes generados en un cierto nodo origen puedan ser encaminados y retransmitidos por distintos nodos retransmisores hasta llegar al nodo destino a través del medio inalámbrico, aunque origen y destino no se encuentren dentro del rango de transmisión directo. En cada una de las retransmisiones, los paquetes de datos “saltan” de un nodo a otro, avanzando hacia su entrega en el destino (transmisiones *multi-hop* o multi-salto). Como paso previo a la retransmisión y entrega de los paquetes, los nodos deben ser capaces de hallar una ruta entre los nodos origen y destino, la cual determina el camino que seguirán los paquetes a través de la red durante la comunicación. Las rutas se crean y gestionan utilizando algoritmos de enrutamiento, hasta que finalizan tras una eventual

caída de alguno de los enlaces que la componen, o cuando caducan tras una interrupción de la comunicación. Estos procesos de búsqueda de rutas y de retransmisiones exigen la colaboración de los nodos que componen la red. A cambio, los nodos pueden utilizar la red en su propio beneficio, justificando así el empleo de los recursos de los nodos en estas tareas. Sin esta colaboración, la conectividad de la red y su propia existencia se pueden ver seriamente comprometidas. Mientras que en determinados escenarios se puede asumir que todos los nodos acceden a cooperar en estas tareas, en otros es posible que una parte de ellos no lo haga, aunque no por ello dejen de utilizar la red para enviar y recibir los paquetes de datos de su interés. En líneas generales, este tipo de comportamiento anómalo que consiste en descartar los paquetes que el nodo debe retransmitir para otros nodos, al mismo tiempo que se emplea la red para transmitir los propios paquetes, se ha denominado egoísta [36]. Aunque existen otros tipos de ataques y comportamientos anómalos que atañen al campo de la seguridad en redes MANETs, el presente trabajo se ha centrado en el estudio de este tipo de comportamiento.

En este contexto, la comunidad científica ha investigado el comportamiento que pueden presentar los nodos en referencia a su nivel de cooperación, las consecuencias del egoísmo de ciertos nodos, y las técnicas para contrarrestarlo [37]. Dichos estudios se han planteado distintos retos y objetivos: ¿Qué tipo de acciones pueden llevar a cabo los nodos egoístas y de qué modo? ¿Cuál es el efecto de sus acciones sobre las comunicaciones de la red? ¿Podría ser beneficioso un cierto nivel de egoísmo? ¿Qué técnicas podrían implementarse para evitar los efectos negativos o para incentivar la cooperación de los nodos? ¿Cómo comprobar la efectividad de dichas técnicas y su influencia sobre el rendimiento? Este trabajo ahonda en algunas de estas preguntas para tratar de darles respuesta. En un primer momento, se llevó a cabo una extensa revisión de la literatura existente, poniendo especial énfasis en estudiar y comprender los distintos tipos de técnicas de incentivo a la cooperación propuestas en otros trabajos. De entre todas ellas, la potencialidad que ofrecían las técnicas basadas en reputación motivó que la atención de la investigación se centrara en ellas, frente a los demás tipos de técnicas. Las técnicas de reputación se basan en el aislamiento de los nodos egoístas por parte de los demás nodos. Cada nodo utiliza distintas herramientas para detectar a aquellos nodos que no cooperan adecuadamente y evitar que participen como nodos retransmisores (ya que no son fiables y pueden descartar los paquetes) o como orígenes o destino de datos (para incentivarlos a cooperar si quieren beneficiarse de la utilización de la red). Las técnicas basadas en reputación son relativamente fáciles de implementar, con unos requisitos asumibles y factibles y buenas expectativas en cuanto a su rendimiento. A partir de su estudio, aparecieron diversas cuestiones que motivaron la investigación realizada: ¿Cuál es el rendimiento esperable de estas técnicas? ¿Han sido evaluadas correctamente en los estudios publicados? ¿Qué posibles anomalías se pueden detectar en su funcionamiento?

¿Es posible solventar estas anomalías? Estas preguntas y los resultados obtenidos tras la finalización de cada fase fueron guiando los pasos de la investigación cuyos frutos se plasman en esta tesis. Para sintetizar las líneas principales seguidas, se enumerarán a continuación los objetivos y contribuciones alcanzados tras la realización de esta tesis, siguiendo el orden en el que fueron desarrollados:

- Implementación y análisis de técnicas de reputación propuestas en otros trabajos de la literatura para el estudio comparativo de su rendimiento frente a otras técnicas propuestas en este trabajo.
- Dimensionamiento de las condiciones y los procedimientos apropiados para la evaluación realista de las técnicas de reputación en una red MANET con presencia de nodos egoístas.
- Demostración de la importancia de la precisión de los modelos de canal radio en la evaluación del rendimiento de las técnicas de reputación.
- Propuesta y análisis de diferentes métodos de compensación que combaten los efectos negativos producidos por las colisiones de paquetes y los errores de transmisión sobre la capacidad de detección de las técnicas de reputación.
- Propuesta y estudio comparativo de técnicas de detección que superan en términos de rapidez y precisión en la detección a las técnicas más tradicionales como las bayesianas.
- Propuesta de técnicas que logran alcanzar los objetivos de rendimiento planteados: aislamiento efectivo de los nodos con un comportamiento egoísta y salvaguarda y aumento de la conectividad de los nodos cooperativos.
- Aprovechamiento eficiente de las características complementarias que los sistemas de comunicaciones celulares ofrecen respecto a las redes MANET puras para facilitar la detección y el aislamiento de los nodos no cooperativos.

Se ofrece en los siguientes párrafos una panorámica que describe la estructura de la tesis para introducir al lector en los temas que serán tratados. Se presenta de manera resumida el contenido de cada uno de ellos y las líneas de la investigación que los interconectan.

Excluyendo los capítulos de Introducción y Conclusiones, el resto de capítulos que componen esta tesis pueden agruparse en dos grandes bloques, atendiendo a si presentan o no resultados de investigación. En el grupo de los capítulos que no presentan resultados de investigación se incluyen los capítulos 2 al 4. El propósito de los capítulos de este primer bloque es el de servir como referencia de información para comprender los procedimientos utilizados en los capítulos que contienen resultados de investigación. En ellos se resumen los conocimientos previos aconsejables para poder entender las

contribuciones de la presente tesis, con el objetivo de que puedan ser consultados en caso necesario. El resto de capítulos, del 5 al 8, contienen las aportaciones originales del trabajo. El último capítulo sintetiza gran parte de los aspectos tratados en los capítulos anteriores.

El capítulo 2 inicia el bloque de capítulos previos a los resultados. Constituye un resumen exhaustivo de los estudios sobre técnicas de incentivo a la cooperación extraídos de los trabajos más sobresalientes de la literatura en este campo en la pasada década. El capítulo parte de los términos más generales del problema para después introducir al lector en aspectos más específicos de este trabajo como las técnicas de reputación, las distintas técnicas de detección de comportamientos egoístas, etc. Al mismo tiempo, se complementa la información anterior con las pertinentes justificaciones de las decisiones llevadas a cabo durante el trabajo que fueron acotando las áreas de interés a investigar.

En el capítulo 3 se incluyen a modo de referencia los conocimientos sobre redes inalámbricas necesarios para poder entender mejor el presente trabajo. Se centra en dos tipos específicos de redes: las redes MANET y las redes móviles celulares. Dentro de esta división, en el apartado de redes MANET se hace especial hincapié en los aspectos relacionados con el enrutamiento, centrándose en el protocolo de enrutamiento DYMO (*Dynamic MANET On-demand*), por ser utilizado en los procesos experimentales de evaluación de resultados mediante simulación en este trabajo. Por otro lado, el apartado de redes celulares trata las redes HSDPA (*High-Speed Data Packet Access*) y los aspectos de las mismas que han sido utilizados en el proceso de evaluación de resultados.

El capítulo 4 introduce al lector en la plataforma de simulación de redes ns-2, que ha sido la herramienta escogida para la evaluación experimental de las técnicas propuestas e implementadas en el presente trabajo. En este capítulo se explican las principales características de ns-2, su arquitectura y el procedimiento utilizado para llevar a cabo los experimentos que han validado los resultados de la tesis. En cuanto a su estructura, se detallan aspectos importantes para el presente trabajo tales como la capa MAC (*Medium Access Control*), la capa física y los relacionados con la parte inalámbrica de la red, como el canal radio y los modelos de propagación. Este último aspecto será fundamental en los siguientes capítulos de resultados.

El capítulo 5 es el punto de partida del bloque de capítulos de resultados y motivará en gran parte el resto del trabajo. En él se llevó a cabo un estudio de dimensionamiento con el propósito de analizar el rendimiento de algunas técnicas de reputación en diferentes condiciones de operación y comunicación para establecer sus límites e identificar sus potenciales debilidades. Se introduce la técnica de observación *watchdog* así como las técnicas de reputación de Marti [40] y TEAM (*Trust tnhanced security Architecture for Mobile ad-hoc networks*) [41], que son utilizadas como técnicas de referencia a lo largo

de la tesis. Se identifican como factores clave del rendimiento de las técnicas de reputación la capacidad de observación de la técnica *watchdog* así como el número de saltos promedio de las transmisiones multi-salto. Se demuestra la importancia de emplear un modelo de canal realista para un correcto estudio de ambos factores. Al evaluar las técnicas de reputación en condiciones realistas, se muestra el importante deterioro de su rendimiento en términos de conectividad de la red, lo cual exige la propuesta de técnicas que contrarrestren este deterioro.

A partir de los resultados del capítulo 5 se constató que gran parte del deterioro del rendimiento observado al evaluar las técnicas de reputación en condiciones realistas procedía de que la técnica de observación *watchdog* tenía un comportamiento anómalo provocado por colisiones de paquetes en el canal radio o errores de transmisión. Esto generaba un gran incremento del número de acusaciones incorrectas de las técnicas de reputación. En el capítulo 6 se proponen tres técnicas que tienen como objetivo compensar la inexactitud de *watchdog* y rebajar el nivel de acusaciones incorrectas para mejorar la conectividad de las redes MANET. Cada propuesta consigue este objetivo mediante una estrategia diferente: RAM (*Reset Activity Mode*) incrementa la importancia del comportamiento cooperativo de los nodos, RFM (*Reset Failure Mode*) combate la disminución de reputación que pueden provocar las caídas del enlace radio, y WM (*Warning Mode*) proporciona una oportunidad extra a los nodos acusados para comprobar si realmente su comportamiento es egoísta y evitar así que nodos cooperativos sean acusados por la inexactitud de la técnica *watchdog*. Los resultados demostraron la capacidad de las técnicas para reducir el número de acusaciones incorrectas, e incrementar la disponibilidad de rutas multi-salto seguras, lo cual propicia un aumento de la conectividad en redes MANET en presencia de nodos egoístas.

El capítulo 5 mostró que el funcionamiento anómalo de las técnicas de reputación procedía de los errores de la técnica *watchdog* que afectaban al proceso de detección de los nodos egoístas. El capítulo 7 analiza pormenorizadamente distintas técnicas de detección, cuya misión, dentro de las técnicas de reputación, es decidir si un nodo debe o no ser acusado. Las técnicas de detección bayesianas propuestas en la literatura, tratan de robustecer a la técnica *watchdog* original para que sea menos sensible al error introducido por el canal de transmisión radio. Además, el capítulo introduce un modelo más generalista de nodo egoísta, en el que se descartan no todos los paquetes que deben retransmitir, sino sólo una fracción de ellos, de manera aleatoria. Con esta generalización resulta más difícil la detección de los nodos, dado que el comportamiento egoísta del nodo puede estar enmascarado por los errores de detección de la técnica *watchdog*. En el capítulo se demuestra el compromiso existente entre la velocidad y la precisión del proceso de detección [138]: tomar decisiones correctas de acusación o no acusación requiere un cierto número de observaciones por parte de la técnica *watchdog*. Sin

embargo, aumentar el número de observaciones puede hacer que los nodos realmente egoístas descarten más paquetes. Este compromiso se hace evidente al evaluar analíticamente el funcionamiento de las técnicas de detección bayesianas. Como alternativa, se propone una técnica de detección basada en un enfoque exponencial en el cual la probabilidad de error de *watchdog* se utiliza de manera explícita, lo cual facilita la selección de sus parámetros de configuración, frente a las técnicas tradicionales bayesianas. Los resultados presentados demuestran que en las condiciones simuladas, la técnica exponencial obtiene el mejor rendimiento en términos de precisión, con un menor coste en paquetes descartados antes de la detección, es decir, con un menor retardo de detección. También se investigó la importancia de utilizar una buena estimación de la probabilidad de error de la técnica *watchdog* y los efectos de la desviación en la estimación de este parámetro.

El capítulo 8 presenta dos técnicas de reputación que explotan la capacidad de la infraestructura de red celular para apoyar los procesos de detección de nodos egoístas y su aislamiento en una red multi-salto celular. Las técnicas propuestas demuestran las considerables ventajas derivadas de la utilización de la infraestructura celular como sistema de apoyo para las técnicas de reputación y de detección de nodos egoístas. Sin este apoyo, las técnicas de reputación no consiguen aislar correctamente a los nodos egoístas, debido a que su identidad sólo es conocida por el entorno del nodo que los detecta y por ello sólo es posible un aislamiento local del nodo, el cual no es suficiente para reducir apreciablemente la conectividad de los nodos egoístas. La primera técnica, BC (*Broadcast Category*), tiene como objetivo hacer pública la información local de la identidad de los nodos que son detectados como egoístas para alcanzar un verdadero aislamiento de los mismos. Por otro lado, la segunda técnica, SC (*Selfishness Check*), trata de reducir las posibles acusaciones incorrectas a nodos cooperativos, que quedarían completamente aislados en la red. Los resultados obtenidos muestran que no es posible aislar a los nodos egoístas empleando únicamente técnicas de reputación como TEAM en las que la información de reputación se difunde sólo a nivel local. Asimismo, se demuestra que al emplear las dos técnicas propuestas conjuntamente se consigue aislar satisfactoriamente a los nodos egoístas, así como preservar la conectividad de los nodos cooperativos, todo ello con la introducción de un coste mínimo en términos de mensajes de señalización intercambiados con la entidad central en el interfaz celular.

Finalmente, el capítulo 9 resume las principales aportaciones del presente trabajo y discute cuáles son las líneas de investigación que parten de estas conclusiones y que podrían ser exploradas en el futuro.

UNIVERSITAS
Miguel
Hernández

2

Técnicas de incentivo a la cooperación

El presente capítulo presenta el estado del arte de la investigación en técnicas de incentivo a cooperación y técnicas de reputación en redes inalámbricas, con el fin de establecer el contexto en el que se sitúa esta tesis doctoral e ilustrar los motivos de su realización. Se parte de los aspectos más generales de redes MANET, para después discutir los distintos tipos de comportamientos y ataques por parte de los nodos que han sido estudiados en la literatura. Se enumeran las distintas categorías de estrategias de incentivo a cooperación propuestas en trabajos anteriores, y se analizan las ventajas, aplicaciones e inconvenientes de cada una. Se presentan entonces las técnicas basadas en reputación, en las cuales se centra esta tesis. Se introducen distintas técnicas de observación, y en especial la técnica *watchdog*. A continuación se discute acerca de la viabilidad de las técnicas de reputación y de las condiciones de simulación empleadas en distintos trabajos para su evaluación. Dentro de las técnicas de reputación, se recopilan las técnicas de detección más destacadas. Las técnicas de detección son aquellas que permiten decidir si un nodo debe o no ser acusado de mantener un comportamiento egoísta. Finalmente, se citan algunos trabajos anteriores en los cuales se proponen

técnicas de reputación que utilizan algún tipo de entidad central como asistente al proceso de detección y aislamiento de los nodos egoístas.

2.1 Cooperación en redes MANET

Los nodos que componen una red MANET se comunican entre ellos directamente, o bien indirectamente a través de varios saltos utilizando a otros nodos como retransmisores. No requieren una jerarquía o infraestructura de red fija que realice las funciones necesarias para el mantenimiento de la red, sino que dichas funciones deben ser asumidas y realizadas por los propios nodos, que suelen estar limitados por recursos escasos como la batería, la capacidad de computación y comunicación, etc. Algunos de los nodos pueden desviarse del comportamiento cooperativo que consiste en seguir estrictamente los protocolos establecidos para la comunicación. La literatura sobre MANETs ha estudiado diferentes tipos de comportamiento de los nodos que no siguen los protocolos, denominados en general nodos no cooperativos (aunque determinados comportamientos no cooperativos reciben nombres más específicos), y también ha estudiado posibles soluciones que tratan de evitar los perjuicios que pueden causar a la red y a las comunicaciones de los demás nodos [62]. Este capítulo está dedicado a enumerar y analizar los distintos trabajos sobre el tema publicados en la pasada década. En primer lugar, se discutirán en la siguiente sección los distintos comportamientos no cooperativos que han sido estudiados en dichos trabajos.

2.1.1 Tipos de comportamiento no cooperativo

Los trabajos dedicados a la cooperación de los nodos en redes MANETs estudian diferentes comportamientos posibles. Algunos de ellos proponen clasificaciones de estos comportamientos y de los potenciales ataques por parte de los nodos. En algunos además se discuten también las motivaciones de los nodos o de sus usuarios para justificar un cierto patrón de comportamiento. Ante la falta de uniformidad, [36] propone especificar los tipos de comportamiento según distintos parámetros: tiempo (durante cuánto tiempo existe el comportamiento), grado (qué probabilidad p hay de que se produzca), nivel (a nivel de datos o de control), tipo (qué acción se ejecuta) y hacia quién (qué nodo o nodos sufren la acción). A continuación se enumeran las distintas clasificaciones propuestas sobre tipos de comportamiento en los trabajos que fueron consultados por el autor. Asimismo, la Tabla 2-1 al final de esta sección ofrece una recopilación a modo de resumen de dichos trabajos destacando el comportamiento no cooperativo en el que han centrado su atención.

A pesar de que la terminología referente al comportamiento no cooperativo de los nodos varía en los distintos estudios, hay ciertas convenciones generalizadas. En primer lugar, los nodos cooperativos son aquellos que siguen estrictamente las directrices de los protocolos establecidos para la comunicación, ejecutando todas las tareas de enrutamiento, retransmisión de paquetes, acceso al medio, etc. En cuanto al comportamiento no cooperativo, existe un amplio acuerdo en llamar nodos egoístas a aquellos que no siguen los protocolos en sentido estricto, sino que dejan de realizar alguna tarea, con el objetivo de ahorrar cierto recurso (batería, capacidad de computación) u obtener alguna ventaja sobre el resto de nodos. Sin embargo, cualquier intencionalidad de perjudicar directamente al resto de nodos está excluida de la definición de nodo egoísta, entrando ya dentro del término de comportamiento malicioso, explicado más adelante. Uno de los primeros trabajos en ocuparse del egoísmo de los nodos y en acuñar este tipo de comportamiento fue Marti [40]. En [40], el comportamiento egoísta consistía en que el nodo participaba en las tareas de enrutamiento, pero luego no retransmitía los paquetes que le eran encomendados. La motivación de estos nodos egoístas es ahorrar recursos como la batería, capacidad de computación, etc [61]. Como veremos más adelante, este no ha sido el único comportamiento de tipo egoísta estudiado. Por otro lado, los nodos maliciosos son aquellos que ejecutan acciones para perjudicar intencionadamente al resto de nodos, aún a costa de tener que hacer uso de sus propios recursos para ello. Los nodos maliciosos generalmente ejecutan ataques de distintos tipos, contra los cuales se hace necesario implementar exhaustivos sistemas de seguridad de red, con la dificultad añadida que suponen las características especiales del medio de transmisión inalámbrico frente a otros sistemas de transmisión. Los tipos de ataques ejecutados por nodos maliciosos pueden ser muy variados: *black hole* o *grey hole* [36], *spoofing*, *denial of service*, suplantación de identidad, etc. Existe por tanto un consenso en los trabajos que utilizan esta clasificación en nodos cooperativos, egoístas y maliciosos, entre los que cabe citar [58], [36], [59], [64], etc. En concreto, [36] añade una categoría, la de los nodos inactivos. Un nodo inactivo es aquél que no participa en ninguna tarea relacionada con la red, ni a nivel de datos ni a nivel de control. Tampoco son origen ni destino de datos, y por tanto su única influencia en la red podría ser aumentar o disminuir la densidad de nodos cooperativos. [59] señala que los nodos que desconectan la interfaz radio (se denominarán nodos desconectados) son capaces de ahorrar más energía que los nodos egoístas convencionales. Es decir, es mejor desconectar completamente el interfaz radio cuando no está interesado en mandar o recibir mensajes, que retransmitir sólo mensajes de control y descartar los mensajes de datos. Sin embargo, a pesar de que es una buena estrategia para ahorrar batería, en una red MANET parece difícil saber exactamente los momentos en que se va a necesitar la interfaz radio para recibir o transmitir mensajes. De modo similar, [63] pone en duda que el comportamiento egoísta tradicional de no retransmitir paquetes de datos pero sí

paquetes de control, pueda ser útil para ahorrar energía, puesto que la energía gastada cuando el nodo está inactivo pero con el interfaz radio conectado podría no ser despreciable frente a la energía gastada en tareas de retransmisión, como se había considerado en los estudios hasta la fecha. Aún así, se espera que la mayor parte de los problemas causados por nodos no cooperativos en las redes MANETs se deba a la acción de los nodos egoístas, y no a la de los nodos maliciosos o fallidos[2] [63].

Existen otros estudios que, dentro del comportamiento egoísta, plantean distintos patrones. En [34], los nodos egoístas se dividen en dos tipos: los que participan en la fase de búsqueda de ruta pero no en la de retransmisión de los paquetes (*tipo 1*), y los que no participan en ninguna de las dos, y sólo transmiten cuando tienen datos propios que mandar (*tipo 2*). La motivación para que los nodos se comporten de esta manera es poder estar conectados (por ello mantienen las funciones de enrutamiento, para permanecer asociados a la red) y enviar o recibir sus propios paquetes pero evitar la retransmisión de paquetes para otros usuarios. En este contexto, [34] considera que el impacto en el rendimiento de los nodos que no participan ni en el enrutamiento ni en la retransmisión es muy bajo (medido en términos de *throughput*[3]). Por ello, como se verá más adelante, en esta tesis se ha optado por estudiar únicamente el comportamiento de los nodos que participan en la fase de búsqueda de ruta pero no en la retransmisión de los paquetes. [58] hace una clasificación más exhaustiva del comportamiento egoísta. En concreto, hace referencia a cuatro posibles acciones: a) no retransmitir mensajes RREQ[4], b) no retransmitir mensajes HELLO[5], c) retrasar intencionadamente la retransmisión de los mensajes RREQ, d) retransmisión de mensajes de enrutamiento pero no los mensajes de datos con origen o destino en otros nodos. Este último tipo de comportamiento es el que centra la atención de la gran mayoría de los trabajos publicados sobre cooperación en redes MANET [37] y también de esta tesis. Dentro de este tipo de egoísmo, cabe además la posibilidad de distinguir, siguiendo las indicaciones de [36] sobre aspectos del comportamiento egoísta antes mencionados, entre nodos que descartan todos los paquetes que deberían retransmitir (*black hole atack*) y nodos que descartan únicamente una parte de ellos, decidiendo de manera aleatoria cuáles descarta con una cierta probabilidad[6] p

[2] Nodo fallido se refiere a un dispositivo que por algún defecto en su parte software o hardware no realiza correctamente las tareas colaborativas que especifican los protocolos de redes MANET.

[3] El *throughput* es un parámetro de rendimiento de la red utilizado como medida de la calidad de servicio percibida por el usuario que se calcula generalmente dividiendo el número de bytes transmitidos correctamente por unidad de tiempo

[4] RREQ (*Route REQuest*) es el acrónimo de un tipo de mensajes utilizado en la mayoría de los protocolos de enrutamiento reactivos para llevar a cabo el proceso de búsqueda de rutas. Cuando un nodo desea transmitir un mensaje a otro nodo y no dispone en su tabla de rutas de información sobre la ruta a seguir para encaminar al nodo, inicia un proceso de búsqueda de rutas transmitiendo un mensaje de RREQ que será retransmitido por otros nodos hasta alcanzar finalmente el nodo destino.

[5] HELLO es otro tipo de mensajes utilizados en algunos protocolos de enrutamiento en MANETs. Su misión es informar a los nodos vecinos de que el nodo que transmite el mensaje de HELLO está dentro de su alcance de transmisión radio.

[6] En el capítulo 7 se asumirá este patrón de nodo egoísta que descarta paquetes de manera aleatoria con una cierta probabilidad, que se denominará p_s.

(*gray hole atack*). Este es el patrón de nodo egoísta adoptado en algunos trabajos ([38] y [139]). [33] propone un patrón de comportamiento egoísta en el que los nodos modifican su grado de egoísmo en función de la energía restante en su batería. De esta manera, si la energía es suficiente, la probabilidad de que el nodo actúe egoístamente tiene cierto valor $p<1$, pero si la batería es menor que cierto umbral, entonces el nodo adopta un comportamiento egoísta continuo $p=0$. También atendiendo al nivel de batería del terminal, en [102] se proponen tres modelos de nodos egoístas: los que descartan los paquetes de datos pero participan en la fase de establecimiento de rutas (primera clase), los que descartan tanto los paquetes de datos como los de establecimiento de ruta (segunda clase), y los que actúan según su nivel de carga de batería. Si el nivel es óptimo se comportan como nodos cooperativos. Al descender el nivel se convierten en nodos de la primera clase, y si baja de cierto umbral, entonces se convierten en nodos de la segunda clase. En los estudios que emplean la teoría de juegos para evaluar los comportamientos de los nodos y las técnicas de incentivo a cooperación, que serán comentados más adelante en la sección 2.2.2, el comportamiento egoísta o cooperativo de cada nodo viene determinado por la función de utilidad considerada, que establece qué beneficio piensa el nodo que va a percibir según la estrategia que escojan él y los demás nodos. Este tipo de comportamiento no cooperativo se suele denominar racional, ya que cada nodo evalúa en cada caso si le conviene o no cooperar [76]. La Tabla 2-1 muestra una clasificación de los posibles tipos de comportamiento no cooperativo estudiados en la literatura.

Tipo de comportamiento	Referencia
Malicioso	[36]
Variable en función de la batería	[33] [102]
Descarte aleatorio de paquetes (*gray hole*)	[38] [88] [39][133][118]
Descarte de paquetes de datos (*black hole*)	[36] [40] [58] [63] [34] [37][60] [39]
Inactivos	[36] [58] [59] [60]
Desconectados	[58] [59]
No retransmiten mensajes HELLO	[58]
Racional	[76][93][88][35]

Tabla 2-1. Tipos de comportamiento no cooperativo.

2.1.2 Efectos del comportamiento egoísta

La aparición de nodos egoístas en la red desencadena ciertos efectos que pueden ser percibidos por los usuarios como una reducción del rendimiento y de la calidad de servicio recibida. A nivel de red, se aprecia una reducción de la conectividad, pudiendo llegar a aparecer segmentos de la red inconexos entre sí. La intensidad de esta reducción dependerá del porcentaje de nodos egoístas en la red, de su distribución, de su grado de egoísmo, del tipo de acciones egoístas que se ejecutan y de la aplicación de algún tipo de técnica de prevención de egoísmo. Otros factores como el tamaño de la red y la densidad de nodos también pueden influir en la intensidad de los efectos del egoísmo (capítulo 5). [58] cita como posibles efectos de los nodos egoístas el aumento del número de saltos de las transmisiones multi-salto y la reducción del *throughput*. Igualmente señala que la eficiencia de la comunicación se deteriora, hasta que se hace inviable cuando la proporción de nodos egoístas frente a los nodos cooperativos es demasiado alta. Por otro lado, [36] señala que mientras que el efecto de los nodos egoístas que retransmiten sólo paquetes de control pero no de datos (nodos egoístas) puede ser muy perjudicial, el daño que causan los nodos denominados inactivos (no retransmiten ni paquetes de control ni de datos que no sean de su propio interés) es solo moderado. En otro estudio se muestra incluso que la existencia de nodos desconectados (nodos que desconectan la interfaz radio cuando no tienen datos que recibir o transmitir) puede ser beneficiosa en redes muy densas, ya que tiene un impacto muy positivo al reducir la sobrecarga generada por los mensajes de control y enrutamiento, y por tanto también el consumo de energía tanto para los nodos desconectados como para los nodos cooperativos [59].

2.2 Técnicas de incentivo a la cooperación

En la literatura se han propuesto técnicas para combatir el egoísmo de los nodos y tratar de incentivarlos a cooperar en la retransmisión de los paquetes. Tradicionalmente se han dividido en tres conjuntos principales: técnicas de reputación, técnicas de crédito y técnicas basadas en teoría de juegos, si bien en un cuarto conjunto se podrían agrupar aquellas propuestas que no encajan en las anteriores [37]. En las técnicas de reputación, cada nodo observa el comportamiento de sus vecinos en cuanto a si realizan o no las tareas que le son encomendadas, y utilizan esta información para distinguir si son nodos fiables y predecir su comportamiento futuro. Por otro lado, los esquemas basados en crédito emplean una moneda virtual que puede corresponderse o no con un valor monetario real, para compensar a aquellos nodos que accedan a realizar la retransmisión de paquetes. Además, los nodos necesitan también este crédito para mandar sus propios paquetes. Finalmente, la teoría de juegos modela el proceso de retransmisión como un

juego donde cada uno de los nodos, supuestamente racionales, modifica su estrategia para optimizar su propio beneficio, que es la transmisión de sus propios paquetes a costa del menor gasto de energía. En esta sección se exponen cada uno de estos enfoques y los estudios correspondientes, excluyendo las técnicas basadas en reputación, que son tratadas con más detalle en el siguiente apartado por su especial relevancia en este trabajo. En cada una de las categorías de técnicas de incentivo a cooperación se detallan sus principios de funcionamiento, sus requisitos, sus ventajas e incovenientes, y se mencionan algunas de las principales propuestas.

2.2.1 Técnicas basadas en crédito

[64] introdujo por primera vez el concepto de transacción comercial en su modelo de incentivo a cooperación. En términos generales, todos los sistemas basados en crédito siguen una estrategia parecida: un nodo que proporciona servicio a otros nodos recibe una cierta compensación en forma de crédito, mientras que por otro lado se aplica cierto gravamen a aquellos nodos que se benefician de este servicio, que pueden ser el origen y/o el destino. En su aportación, [64] propone dos estrategias ligeramente diferentes: el modelo PPM (*Packet Purse Model*) y el modelo PTM (*Packet Trade Model*). En ambos, los nodos que retransmiten paquetes para otros nodos reciben una moneda virtual llamada *nuglet*, que a su vez gastan los nodos que actúan como destinos o como orígenes de dichos paquetes. Dependiendo del modelo variará la forma de cobrar a los nodos receptores del servicio. Por un lado, en el modelo PPM, el nodo origen deposita los *nuglets* necesarios en el paquete y los nodos intermedios se los cobran al mismo tiempo que realizan la retransmisión. Se descartan aquellos paquetes que no contengan *nuglets* suficientes, por lo que el nodo origen debe saber exactamente cuántos *nuglets* debe emplear para llegar a su destino. De ahí que este esquema únicamente pueda aplicarse en protocolos de enrutamiento en origen como DSR (*Dynamic Source Routing*) y tenga que excluirse en otros como AODV (*Ad-hoc On-demand Distance Vector*) [7]. Además, los nodos intermedios pueden cobrarse más *nuglets* de los que se acuerde, o bien podrían cobrarlos y no retransmitir correctamente los datos, ya que no hay ningún mecanismo que lo asegure. Por otro lado, en PTM cada nodo intermedio compra los paquetes al nodo anterior por un precio y los vende al siguiente a un precio mayor, siendo la diferencia su compensación por la retransmisión. Al final, el nodo destino es el que debe pagar el precio más alto a su predecesor. A pesar de que PTM no está limitado a protocolos de enrutamiento en origen, es sin embargo vulnerable a ataques del tipo DoS (*Denial of Service*) ya que los nodos pueden generar y transmitir paquetes sin tener que pagar ninguna tasa por ello. Además, ambos métodos tienen otra limitación importante, que es la cuestión de cómo validar la autenticidad de los *nuglets*. Los nodos pueden reutilizar los *nuglets* empleados en retransmisiones anteriores, así como aumentar su número de

nuglets a su antojo. Contra esta posibilidad se sugiere la comercialización de nodos con un módulo de seguridad a prueba de manipulaciones incluido en un chip o tarjeta de seguridad, lo cual sin embargo dificulta su aceptación comercial. Otro trabajo [65] emplea un algoritmo de clave pública en el módulo de seguridad, y muestra como cada nodo puede maximizar sus beneficios empleando alternativamente PPM o PTM en una red con nodos egoístas. Además, muchos trabajos siguen la filosofía de intercambio de *nuglets* de [64], por ejemplo [74]. [75] compara el rendimiento de ambos enfoques.

[66] evita los problemas del cálculo inicial de *nuglets* variando ligeramente la técnica PPM anterior. Su técnica consiste en dos fases: descubrimiento de rutas y transmisión de datos. En la fase inicial, el nodo destino calcula la cantidad de crédito que debe pagarse a los nodos intermedios, y lo notifica al nodo origen o bien a una autoridad bancaria central. En este caso, el pago se realiza automáticamente durante la transmisión de los datos. Sin embargo, este esquema depende exclusivamente de la fiabilidad del cálculo del pago realizada por el nodo destino, de manera que si el cálculo no se realiza correctamente, los nodos intermedios no recibirán su compensación. El nodo destino podría negarse a informar a la autoridad central sobre los pagos a los nodos intermedios por dos motivos. En primer lugar, se necesita gastar energía para informar al banco central. En segundo lugar, para pagar a los nodos intermedios, el banco central descuenta cierta cantidad equitativa a todos los nodos de la red. Por ello, si un nodo destino no informa de que la autoridad central debe pagar a los nodos intermedios, tampoco se cobrará el crédito a ninguno de los nodos, ni siquiera al nodo destino.

Para evitar los problemas de la falta de colaboración de los nodos en la transmisión correcta de los recibos, SPRITE (*Simple, cheat-PRoof credIT-based system*) [67] introduce la idea de una entidad central de control, seguida por muchas otras propuestas de técnicas basadas en crédito [80]. SPRITE también emplea una moneda virtual, y evita el uso de un módulo de seguridad en el equipo del usuario, aunque requiere una autoridad central llamada CCS (*Credit Clearance Service*) para mantener el balance de créditos, que debe consistir en un sistema autónomo externo a la propia MANET. Cada nodo guarda un recibo siempre que recibe un paquete, y lo notifica a la autoridad central cuando dispone de una conexión adecuada. Una vez que se reciben los informes, el CCS debe compensar tanto al nodo que notifica los informes como a los nodos intermedios, así como cargar cierta cantidad al nodo origen. Sin embargo, esta cantidad no es siempre equivalente a la cantidad otorgada a los otros nodos, dado que el CCS deduce más créditos al nodo origen que lo que otorga a los demás, de manera que no es rentable mentir con recibos falsos. Por tanto, SPRITE está a salvo de informes falsos y de ataques de nodos coaligados, dado que ninguna de estas estrategias consigue proporcionar más créditos a los nodos. Sin embargo, dado que cada paquete genera un informe que debe enviarse a la CCS y que cada informe debe ir encriptado con un par de claves pública y

privada, la escalabilidad puede ser un problema. Además el camino entre origen y destino debe conocerse para cargar adecuadamente al origen, con lo cual sólo se pueden emplear protocolos de enrutamiento en origen.

[68] aplica el esquema de créditos a un escenario de redes celulares multi-salto (que ocuparán el capítulo 8 de este trabajo). En este tipo de redes, además de las conexiones celulares tradicionales, los nodos pueden realizar conexiones hacia las estaciones base fijas utilizando a otros nodos móviles como retransmisores, como es el caso típico en las redes MANET. Cada estación base mantiene una ruta a cada nodo de su propia celda. Una vez que el paquete alcanza la estación base, el operador reduce tantos créditos de la cuenta del nodo origen como deban ser otorgados a los nodos retransmisores. Como la estación base tiene información exacta sobre la ruta hacia cada nodo, el número de créditos puede contabilizarse de manera precisa. Cuando el paquete llega al destino, éste responde con una confirmación a la estación base. En previsión de que el destino se niegue a enviar la confirmación para ahorrar energía, la estación base deduce cierta cantidad de créditos de la cuenta del destino antes de enviarle el paquete, y a su vez se los devuelve una vez recibida la confirmación. Se emplea criptografía simétrica para proteger la comunicación entre los nodos y las estaciones base. Este esquema requiere la participación global de todos los nodos en la técnica de incentivo a cooperación. Sin embargo, una MANET real está formada por nodos heterogéneos y puede que algunos de ellos no estén diseñados para reconocer la existencia de un método de pago de créditos. Además, algunos nodos puede que no consigan suficientes créditos debido a que por un mal posicionamiento dentro de la celda nadie los necesite como retransmisores.

Para hacer frente al problema de la escasez de créditos provocada por una localización desfavorable, Raghavan [69] propone dos servicios de retransmisión: uno con prioridad bajo pago y otro gratuito *best effort*. Los nodos intermedios por su parte retransmiten primero todos los paquetes prioritarios antes de transmitir el tráfico *best effort*. A su vez, este comportamiento es observado por sus vecinos de manera promiscua, a la manera de los esquemas basados en reputación (explicado más adelante). Si los vecinos observan que no se respeta la prioridad del tráfico, el pago por los servicios de retransmisión prioritaria es nulo. Para gestionar los créditos de todos los nodos móviles, se utiliza la autoridad central CCS de [67] con la ligera diferencia de que aquí la autoridad CCS es un nodo móvil cualquiera, mientras que en el sistema SPRITE su función era desempeñada por una entidad fija. Además, no se esclarece como un nodo móvil estándar puede registrar los créditos del resto de nodos móviles. En [70], las tareas de selección de ruta y enrutamiento se deciden según cierto parámetro de precio de congestión gestionado por ciertos nodos con mayor jerarquía. Cada nodo negocia cuánto está dispuesto a pagar por la retransmisión según la potencia y el ancho de banda disponibles. Sin embargo, no hay una manera segura de impedir que los nodos declaren precios mayores de lo conveniente.

La mayoría de los esquemas de crédito sólo son compatibles con protocolos de enrutamiento en origen como DSR, dado que necesitan conocer toda la ruta desde el origen al destino. A pesar de que [65] o [69] no lo necesitan, a cambio necesitan la existencia de un módulo de seguridad a prueba de falsificaciones o bien una infraestructura de BS, lo cual no siempre existe en un entorno MANET. PIFA (*Protocol-Independent Fairness Algorithm*) [71] es sin embargo compatible con cualquier tipo de protocolo de enrutamiento. Requiere un servidor central llamado CM (*Central Manager*) que mantiene los créditos del resto de nodos y que periódicamente recibe de ellos informes con los mensajes que han retransmitido. El CM verifica la credibilidad de estos informes y recompensa con créditos a los nodos retransmisores. Cualquier nodo fijo puede ser el nodo CM, pero además debe estar gestionado por un administrador confiable. Cuando algunos de los nodos se contradicen en el test de credibilidad que el nodo CM aplica a los informes periódicos, son automáticamente penalizados con multas llamadas NAM (*Numbers of Alleeged Manipulation*). Si superan un número de multas, los nodos son aislados. Por ello, este esquema está a medio camino entre los de reputación y los basados en crédito. Otra técnica interesante basada en crédito es la que se propone en [72], en el cual también los nodos periódicamente envían a una entidad central el informe de las retransmisiones realizadas. La entidad central aplica una técnica de agrupación de pagos para recompensar a los nodos participantes, de manera que no se recompensan todas las retransmisiones sino solamente algunas seleccionadas de manera aleatoria, para mejorar la escalabilidad. La Tabla 2-2 resume las principales características de las técnicas de incentivo a cooperación basadas en crédito en redes MANET de la literatura.

Característica	Referencia
Necesidad de enrutamiento en origen	[64]
Necesidad de módulo de seguridad	[64][65][74][75] [70] [69]
Necesidad de entidad central	[67][80] [66] [68] [69][71][72] [76]
No necesario cálculo previo del pago	[66][65][74][75]
Posible sobrecarga de señalización	[80] [68] [79]
Varias prioridades de servicio	[69]
Negociación de precios	[70]
Créditos limitados por la localización geográfica	[78] [68]

Tabla 2-2. Técnicas de incentivo a cooperación basadas en crédito.

En general, las técnicas basadas en crédito tienen varios inconvenientes [73]:

- En muchas de las técnicas debe estimarse a priori el número de saltos para dotar al paquete en transmisión de un número suficiente de monedas. Si el cálculo no es correcto, algunos paquetes pueden ser rechazados y su reenvío puede ser costoso en términos de energía.
- Pueden necesitar una entidad central confiable que dé veracidad al sistema monetario y gestione la moneda virtual, o algún tipo de módulo de seguridad a prueba de falsificaciones que impida que los nodos modifiquen su crédito fraudulentamente.
- Complejo equilibrio en el cálculo del pago a los nodos retransmisores y el cobro a los nodos extremos (origen y destino).
- La distribución del crédito disponible puede estar más relacionada con la situación geográfica de los nodos que con su egoísmo [78]. Los nodos situados en las afueras no podrán obtener suficiente crédito para sus transmisiones, cuando son los más interesados en ello, en un escenario típico de red multi-salto celular.
- La regulación de la circulación de moneda es compleja: un exceso de moneda provoca que nadie coopere porque todos tienen suficientes, mientras que la escasez de moneda impedirá que se hagan transmisiones.
- Si el número de monedas de cada nodo es reiniciado cada cierto tiempo, se pierde el incentivo de cooperar, puesto que almacenar muchas monedas no sirve de nada tras el reseteo.
- Complejidad de los sistemas de claves para la seguridad de las transacciones [79] [80] [68].
- Un sistema de crédito basado en moneda real pierde atractivo porque habría que pagar por la comunicación (cuando una supuesta ventaja de las redes MANET es que es gratis). Establecer una entidad central de control es también contrario al espíritu de las MANET.
- No está clara la distribución correcta del cobro de monedas entre los nodos interesados en la transmisión (sólo al origen, sólo al destino o a los dos).
- Además, la escalabilidad puede ser un problema grave dado que en redes cargadas el nodo central puede estar sometido a una alta tasa de tráfico en sus inmediaciones además de requerir una gran capacidad de cálculo y de memoria de almacenamiento.
- También, en las soluciones basadas en una entidad central, surge el problema de la sobrecarga de señalización inducida por el intercambio de mensajes de recibos

y pagos entre la entidad central y los nodos, para lo cual se proponen métodos de agrupación de recibos [76].

- Por otro lado, en general, estos sistemas requieren que absolutamente todos los nodos participantes en la red reconozcan y empleen el sistema de crédito establecido, lo cual puede no ser posible en redes realistas.

2.2.2 Técnicas basadas en teoría de juegos

La teoría de juegos es una rama de las ciencias económicas y de las matemáticas cuyo objetivo es analizar las estrategias óptimas de cada jugador racional en competencia con otros jugadores racionales. Las decisiones de todos los jugadores influyen en la utilidad o el beneficio que cada jugador obtiene al final del juego. El objetivo es buscar un punto de equilibrio en donde ningún jugador puede incrementar su propio beneficio cambiando unilateralmente su estrategia (equilibrio de Nash). Estos equilibrios son buscados porque representan una posible solución al problema basada en la estabilidad, es decir, si los jugadores son racionales, no querrán apartarse de esta estrategia puesto que su beneficio no se vería aumentado. La teoría de juegos ha pasado de ser aplicada a problemas de economía social a estudiar un amplio abanico de áreas, incluyendo numerosas aplicaciones en redes de comunicaciones, y en concreto a la cooperación en redes MANET. Se debe señalar que la teoría de juegos asume que todos los jugadores son racionales, es decir, que todos los jugadores buscan su propio beneficio, pero no está tan claro en qué consiste este beneficio, variando de unos estudios a otros. Algunos nodos pueden buscar su beneficio en términos de *throughput* o de paquetes propios transmitidos mientras que otros se concentran en el objetivo de conservar su energía. Asumiendo nodos racionales, la mayoría de los esquemas de teoría de juegos modelan el enrutamiento de paquetes como un juego en el que la estrategia de cada nodo consiste en elegir la tasa de retransmisión que soportará cada nodo, es decir, el número de paquetes que retransmitirá para otros frente al número de paquetes propios que transmitirá [89]. Dado que cada nodo puede cambiar su estrategia con libertad, en el momento en que se detecta un comportamiento egoísta por parte de algún nodo, el resto de los nodos cambiarán su estrategia de cooperación a no cooperación para castigarlo. En función de las condiciones y suposiciones asumidas, el juego convergerá finalmente o no hacia un punto donde todos los nodos estén satisfechos. En este punto de equilibrio, cualquier desviación unilateral de la estrategia de cooperar debe ser penalizada [91]. Puede encontrarse una buena introducción a la teoría de juegos en su aplicación a la cooperación en las redes MANET en [77]. La teoria de juegos, por tanto, sirve para dar un marco matemático formal al estudio de la cooperación en redes MANET [87].

Generous Tit-For-Tat (GTFT) y *multiple-GTFT* (m-GTFT) [88] fueron los primeros esquemas de teoría de juegos propuestos para analizar el problema de la retransmisión de paquetes en MANETs. GTFT se refiere al caso de transmisiones de un solo salto, mientras que m-GTFT generaliza la estrategia para permitir más de una retransmisión por paquete. Estos algoritmos estudian el compromiso entre la energía empleada para retransmitir paquetes de otros nodos frente a la que emplean los otros nodos para retransmitir sus propios paquetes. También se permite la concurrencia de nodos heterogéneos, que se definen como nodos con diferentes restricciones de energía (portátiles, PDAs, móviles, etc.). Cada móvil almacena algunas variables en forma de tablas para decidir si acepta o no la retransmisión de un paquete entrante. Por un lado registra el total de peticiones a otros nodos que han sido satisfactoriamente retransmitidas por estos frente al total de peticiones generadas por el nodo. Por otro lado almacena el total de peticiones que ha retransmitido satisfactoriamente frente al total de peticiones soportado. En cada momento, la retransmisión de un paquete entrante se realiza si se cumplen dos condiciones: el tráfico retransmitido en total durante la sesión no supera el límite total del nodo según su categoría, y además la cantidad de tráfico retransmitido por el nodo para los demás está por debajo de la cantidad de tráfico retransmitido por los demás para el nodo más un cierto parámetro que tiene en cuenta la generosidad del nodo. El trabajo demuestra que bajo estas condiciones se llega a un equilibrio de Nash. Sin embargo, cada nodo requiere reunir una cantidad de información elevada sobre todo el sistema tal como el número de nodos, sus limitaciones de energía, número de peticiones de cada sesión, etc… lo cual parece inviable o poco escalable, a pesar del algoritmo de diseminación de información que se propone. Además, tampoco se especifica cómo se averigua si un nodo ha realizado correctamente la retransmisión o no ni cómo se evita que los nodos transmitan información falseada en su propio beneficio.

Aparece un inconveniente fundamental de las técnicas que aplican el principio de *Tit-For-Tat*: ¿cómo castigar adecuadamente a los nodos que no cooperan, cuando resulta tan difícil distinguir las acciones egoístas deliberadas, como la no retransmisión de un paquete, de los errores de observación de técnicas como *watchdog*, provocadas por errores del canal radio? No son abundantes los trabajos de teoría de juegos que se ocupan de esta cuestión. [95] muestra que en ausencia de técnicas de incentivo, los nodos pueden descartar los paquetes o retransmitirlos con una prioridad baja, y culpar de ello a la poca fiabilidad del canal radio. Se trata de un problema de teoría de juegos con información incompleta ("*hidden information*"). Para hacerle frente, proponen distintos algoritmos con los cuales la utilidad de los nodos se maximiza cuando declaran honestamente su tipo, y actúan de acuerdo a esa declaración. El tipo incluye la prioridad con la que realizan retransmisión de paquetes para otros nodos y el coste en términos de moneda virtual.

A pesar de la popularidad del esquema *Tit-For-Tat*, existen también alternativas a este enfoque. El establecimiento de la red MANET en la técnica propuesta en [80] permite a todos los nodos beneficiarse de ella, pero como ser voluntario para retransmitir tiene un coste, al final todos prefieren esperar y que otro sea el voluntario que establezca la red MANET. Esta circunstancia se estudia entonces aplicando el modelo del "dilema del voluntario".

FAIR [85] combina un algoritmo heurístico con un análisis basado en teoría de juegos. Cada nodo propone un precio por retransmisión realizada. El precio está ajustado para que sea un verdadero mercado en el que los valores altos hacen que descienda la demanda (reduciendo por tanto el número de créditos cobrados), mientras que los valores demasiado bajos la incrementan haciendo que ascienda la demanda y también la energía empleada en realizar las tareas de retransmisión. El precio se ajusta teniendo en cuenta los dos factores: una estimación del precio de retransmisión que cobrará el siguiente nodo según lo observado en ocasiones anteriores y una estimación del coste de retransmisión del paquete, basado en el ancho de banda, la energía y la potencia empleada. Estas estimaciones se calculan con un modelo de estados finitos con realimentación, que determina en qué estado está el "mercado" y la estrategia a seguir. No se establece un cambio a moneda real, y por tanto los créditos no se pueden comprar, sino que sólo se pueden conseguir con retransmisiones.

Catch [84] propone otra estrategia para combatir el egoísmo usando mensajes anónimos para establecer las rutas. Si un nodo no recibe los mensajes anónimos, se pierde la conectividad del enlace. Cada nodo debe tener al menos un enlace para poder enviar sus propios paquetes, pero al no poder saber la identidad del remitente del mensaje, debe responder a todas las solicitudes. La retransmisión de los paquetes se incentiva con un sistema basado en la observación promiscua de paquetes, al estilo de las técnicas basadas en reputación. Se analiza el funcionamiento de la técnica propuesta mediante teoría de juegos. Otros trabajos ponen también de manifiesto la potencia de la teoría de juegos para analizar la estabilidad de técnicas basadas en crédito o reputación, tal como sucede en [84] y [85]. Michiardi [81] analiza el algoritmo de reputación CORE (*COllaborative REputation system)* [82] mediante teoría de juegos cooperativos y no cooperativos. En la primera modalidad, todos los nodos llegan a un compromiso común para actuar coordinadamente en sus estrategias. En la segunda modalidad, la estrategia de cada uno la escoge egoístamente el propio nodo en su beneficio. El más paradigmático modelo de juego no cooperativo es el "dilema del prisionero", cuyo enfoque se aplica aquí. La función de utilidad de cada nodo (el beneficio que obtiene por sus decisiones) se toma como la diferencia entre la energía consumida para transmitir sus propios paquetes, aquellos que él ha originado, frente a la energía consumida para el enrutamiento y la retransmisión de los paquetes de los demás, ponderada por un factor de importancia de la

energía. Todos los nodos tratan de maximizar su beneficio al mismo tiempo que mantienen su reputación.

En esta misma línea de aplicación de teoría de juegos para el análisis de la cooperación en redes MANET se sitúa [83], que se plantea si en una red MANET los nodos deben decidir cooperar o no, aún sin recibir incentivos por ello, y bajo qué condiciones los nodos escogerían la cooperación. Establece un modelo de juego en el que cada nodo, cuando funciona como origen, recibe una utilidad si los paquetes son transmitidos correctamente, y cuando funciona como retransmisor, tiene un coste derivado del número de paquetes que retransmite y el coste de retransmitir cada paquete. La conclusión es que las condiciones para que haya equilibrio cooperativo dependen de la topología de las rutas que se establecen y de las estrategias de los nodos en esa topología. En el escenario estático estudiado, son necesarias técnicas de incentivo para motivar la cooperación de los nodos. Sin embargo, a pesar de que las conclusiones son derivadas matemáticamente mediante teoría de juegos, deben ser cuestionadas debido a las suposiciones y simplicaciones poco realistas que en general realizan todos los estudios basados en teoría de juegos. Otros estudios exploran de manera análoga la potencialidad de la teoría de juegos para averiguar si realmente son necesarios los mecanismos de incentivos a cooperación, y si puede existir ésta sin un incentivo externo [86]. Es una vía interesante pero igualmente adolece de falta de realismo en sus asunciones, en este caso la de suponer un escenario completamente estático y en el que cada nodo sólo puede ser origen de una sola ruta.

Otra aplicación de la teoría de juegos es la de modelar el comportamiento de los nodos egoístas. Como ya se ha mencionado en la sección 2.1.1, [33] propone un patrón de comportamiento egoísta en el que los nodos modifican su grado de egoísmo en función de la energía restante en su batería. La Tabla 2-3 recopila los trabajos de teoría de juegos aplicados al estudio de la retransmisión de paquetes en redes multi-salto.

Característica	Referencia
Aplicación principio *Tit-for-Tat*	[88] [95]
Enfoques alternativos a *Tit-for-Tat*	[80]
Consideran posibilidad error observación	[93] [94] [95]
Análisis de heurística con teoría de juegos	[85][84][81][83]
Exploran necesidad de incentivos	[87]
Asunciones simplistas	[69] [92] [94] [90]

Tabla 2-3. Trabajos y técnicas de incentivo a cooperación que emplean la teoría de juegos.

A pesar de que la teoría de juegos ofrece un marco atractivo y permite derivar conclusiones validadas analíticamente para el estudio de las técnicas de incentivo a cooperación en redes MANET, se ha detectado que muchos tienen en común algunos inconvenientes, que se pueden resumir en la falta de realismo de algunas de sus asunciones básicas, lo cual resta credibilidad y aplicabilidad a sus conclusiones. A continuación se enumeran los principales inconvenientes hallados:

- La mayoría de los estudios suponen que los nodos tienen información completa y en tiempo real de distintas variables del proceso de comunicación, como el número de paquetes no retransmitidos por el resto de nodos, el número de nodos, su grado de cooperatividad o el *throughput* experimentado por el nodo en un cierto intervalo de tiempo, etc. En una red real, y específicamente en las redes MANET, averiguar el valor de dichas variables puede ser una tarea difícil. Aún contando con técnicas para difundir dicha información entre los nodos, el coste en términos de sobrecarga de señalización sería demasiado alto.
- La incertidumbre que los errores de transmisión radio o las colisiones de los paquetes introducen en los procesos de observación que permiten saber a los nodos si sus vecinos son cooperativos o no, puede causar que nodos cooperativos sean injustamente catalogados como egoístas y por tanto sean castigados injustamente. Encontrar una solución a este fenómeno es precisamente una de las motivaciones principales de esta tesis, pero salvo algunas excepciones ([93], [94] y [95]), muchos de los trabajos evaluados parecen obviarlo. [94] introduce la consideración de un canal sujeto a errores que puede provocar que los nodos se acusen unos a otros de egoísmo al aplicar la regla del *Tit-For-Tat*, de manera que al final ningún nodo coopera con los demás y la red sea inoperativa. Por otro lado, [94] adolece de otras asunciones demasiado simplistas.
- Las simplificaciones asumidas para facilitar el análisis mediante teoría de juegos, en cuanto a requisitos que debe cumplir la red, es en determinadas ocaciones excesivo. Algunos trabajos se restringen al estudio de escenarios estáticos, con lo cual las conclusiones derivadas pueden no ser aplicables a escenarios de redes MANET convencionales. Las condiciones asumidas en [92] resultan aún más difíciles de cumplir dado que asume un escenario estático con topología en anillo. Otros trabajos (entre otros [94]) realizan una generalización incorrecta del modelo de juego de dos jugadores repetido[7].
- Con técnicas completamente distribuidas, los nodos establecen relaciones directas de confianza para aceptar o no la retransmisión de paquetes procedentes de otros

[7] El modelo de juego de dos jugadores repetido consiste en que dos agentes racionales deben tomar una decisión en el juego y reciben al final una utilidad en función de las elecciones de ambos. Este proceso se repite indefinidiamente.

nodos. De esta manera, sin un conocimiento previo mutuo, dos nodos racionales no accederían a realizar retransmisiones de los paquetes del otro, incluso aunque ambos fueran nodos que hubieran realizado retransmisiones de paquetes para terceros nodos. En otras palabras, la racionalidad de la teoría de juegos exige reciprocidad directa en el proceso de retransmisión. Esto excluye la posibilidad de que los nodos cooperen y contribuyan a establecer y mantener la conectividad de la red, esperando que otros nodos también cooperen para retransmitir sus propios paquetes, en ese momento o posteriormente, pero que no tienen porqué ser exactamente aquellos a los que el nodo retransmitió anteriormente. En las técnicas basadas en crédito o reputación, y en algunas de las analizadas con teoría de juegos, no se exige esta cláusula de reciprocidad directa. En [90] se asume, además de la reciprocidad directa, que todos los nodos que participan en la red generan un volumen de tráfico similar, lo cual resulta poco realista.

2.2.3 Otras técnicas

Anteriormente se enumeraron las tres grandes categorías de técnicas de incentivo a la cooperación y se discutieron el funcionamiento y los inconvenientes de las técnicas basadas en crédito y las técnicas basadas en teoría de juegos, aplazando la exploración de las técnicas basadas en reputación a la sección 2.3, por su relevancia en este trabajo. A continuación enumeramos algunos trabajos que no encajan estrictamente en ninguna de estas categorías.

Algunas técnicas tienen como objetivo asegurar las transmisiones frente a ataques de nodos maliciosos y de nodos egoístas usando claves de seguridad y criptografía ([74], [103], [104], [105], [106], [107], [108]). El principal inconveniente de estas técnicas es la sobrecarga de señalización introducida por la utilización de las claves para encriptar y asegurar los mensajes. [74] sugiere la utilización de un *token* para la regulación de las retransmisiones. Cada nodo necesita este *token* para poder transmitir sus propios paquetes. Para asegurar la continuidad en la cooperación, el *token* tiene un periodo de validez definido y debe ser renovado periódicamente por los nodos vecinos. Para conseguir el *token*, cada nodo en la red tiene un pequeño trozo de la clave secreta del sistema. Si consiguen suficientes trozos de la clave de los nodos vecinos, pueden renovar su *token*. Sin embargo, la utilización de estos *tokens* requiere una gran cantidad de capacidad de cálculo y de memoria por parte de los nodos móviles.

En [97] se encuentra una interesante propuesta, que no se puede identificar ni con una técnica de crédito o de reputación ni con teoría de juegos. El único nodo que conoce la ruta es el origen, y cada nodo en la ruta está obligado a retransmitir el mensaje, porque mediante un procedimiento especial se consigue que únicamente el nodo destino sepa que

él es el destino. Dado que esto sólo se sabe cuando el nodo llega al final de la ruta, todos los nodos intermedios realizan la retransmisión porque ellos mismos pueden ser el destino. El nodo origen selecciona la secuencia de nodos en la ruta de tal manera que el paquete pasa dos veces por el destino, creando un lazo. Por ejemplo, si la ruta convencional sería Origen–A–B–C–Destino, el nodo Origen selecciona la ruta Origen–A–B–C–Destino–E–Destino. Por otro lado, la parte de datos del mensaje está encriptada con una clave que también va encriptada con una secuencia anidada que se compone de todas las claves públicas de los nodos en sentido inverso. De esta manera cada nodo cuando recibe un paquete intenta ver si es el destinatario descifrando la parte de la clave del mensaje. Si no lo consigue, entonces debe retransmitir el mensaje puesto que aún así podría serlo, debido al lazo creado en la ruta. Es una solución elegante pero costosa por la utilización y el manejo de las claves.

Otros trabajos contienen elementos de distintas categorías de técnicas. En [98] se propone una técnica heurística que mezcla características de técnicas basadas en crédito, teoría de juegos y reputación. Dado que emplear sólo un sistema de crédito puede hacer que los nodos situados en localizaciones favorables hagan muchas retransmisiones y por tanto, al ganar mucho crédito dejen de estar interesados en retransmitir paquetes, se propone adicionalmente penalizar a los nodos que pudiendo hacerlo, no cooperan. En [99], cada cierto periodo de tiempo el nodo destino de un flujo de paquetes envía hacia atrás un mensaje con el número de paquetes recibidos. Cada nodo en la ruta inversa (destino a origen) lo retransmite añadiendo su número de paquetes procesados. El nodo origen puede ver de esta manera qué nodo está comportándose egoístamente (parcialmente sería por tanto una técnica basada en reputación).

La técnica SMT (*Secure Message Transmission*) [104] emplea múltiples rutas redundantes a través de las cuales se envía la información. El mensaje puede ser reconstruido en el destino si llegan satisfactoriamente sólo algunas de las partes enrutadas. Cada una de las rutas recibe una puntuación que responde a su fiabilidad, y las rutas con puntuaciones bajas son excluidas en las siguientes transmisiones. Por tanto, puede asociarse en cierta manera a las técnicas basadas en reputación. [96] también propone que en los mensajes RREQ del protocolo de enrutamiento DSR se propague una lista tabú con la identidad de los nodos egoístas conocidos, lo cual puede ser perjudicial al incrementar la carga de señalización. También propone un tipo especial de mensajes que avisa al destino de la cantidad de paquetes que debe recibir y la velocidad. En caso de que no se cumplan, el destino debe avisar con un mensaje de confirmación negativo. Finalmente, [101] propone evaluar la realimentación sobre la tasa de entrega de extremo a extremo que un protocolo tipo TCP (*Transport Control Protocol*) puede proporcionar para averiguar si algunos nodos del enlace pueden estar descartando paquetes. Para ello, además hay que tener en cuenta que los descartes de paquetes pueden suceder debido a

dos circunstancias: el comportamiento egoísta de los nodos y los factores de la red y el entorno radio como congestión a nivel de red, contención en la capa de enlace de datos y fenómenos de nivel radio como el desvanecimiento. Por ello, [101] propone distintas técnicas para tratar de minimizar los falsos negativos (nodos egoístas que no son detectados) y los falsos positivos (nodos cooperativos que son detectados como nodos egoístas). Como se verá en la siguiente sección y a lo largo de la tesis, este es también uno de los problemas principales a resolver en las técnicas basadas en reputación.

La Tabla 2-4 recopila algunos de los trabajos sobre técnicas de incentivos a la cooperación discutidos en esta sección.

Característica	Referencia
Criptografía	[74], [103], [104][105], [106], [107], [108]
Destino anónimo	[97]
Mezcla de categorías	[98][99]
Múltiples rutas redundantes	[104]
Lista nodos tabú	[96]
Comprobar tasa de entrega extremo a extremo	[101]

Tabla 2-4. Técnicas de incentivo a cooperación pertenecientes a otras categorías.

2.3 Técnicas basadas en reputación

Las técnicas basadas en reputación tratan de detectar a los nodos no cooperativos mediante distintos métodos y de conseguir un consenso entre los nodos de la red para aislar o no utilizar como retransmisores a los nodos no cooperativos identificados. Aislar a los nodos egoístas tiene un doble propósito: no permitir que descarten los paquetes que deben retransmitir, evitando a los nodos detectados como egoístas en los establecimientos de ruta, e incentivarlos a cooperar, dado que si no lo hacen, tampoco podrán usar a los demás nodos como retransmisores. En las técnicas de reputación, distintos métodos sirven a los nodos para obtener información sobre el grado de cooperación de otros nodos y asignarles un determinado nivel de reputación, en función de observaciones directas o indirectas de su comportamiento. La información de primera mano se denomina directa[8], mientras que las recomendaciones o las opiniones de otros nodos suelen denominarse

[8] Esta clasificación no siempre es aplicable. En algunos trabajos, reputación directa se refiere a la que se deriva de observaciones que un nodo realiza vigilando la correcta retransmisión de sus propios paquetes, mientras que indirecta se refiere a la vigilancia de los paquetes de otros, y por último reputación recomendada se refiere a las opiniones de reputación provenientes de otros nodos. Esta terminología se aplicará preferentemente en este trabajo, si no se indica lo contrario.

indirectas. Suelen estar compuestos por dos módulos más o menos identificables: un módulo de monitorización, que registra el comportamiento de los nodos vecinos, y un módulo de reacción, que en función de los informes del módulo de monitorización, asesora al correspondiente protocolo de enrutamiento a la hora de seleccionar las rutas para los paquetes y aislar o no a un vecino, así como retransmitir o no las peticiones de enrutamiento entrantes. Un nodo que se comporte de manera egoísta repetidamente, es decir, que se niegue a retransmitir los paquetes que sus vecinos le envían para retransmitir, acabará obteniendo unos valores bajos de reputación en la opinión de sus vecinos, que reaccionarán bien aislándolo y negándose a retransmitir sus paquetes, o bien evitándolo en sus tablas de rutas, dado que previsiblemente seguirá descartando los paquetes.

La premisa básica sobre la que se asienta la filosofía de las técnicas de reputación es que se puede predecir el comportamiento futuro de los nodos basándose en su comportamiento pasado [109]. Por tanto deben contestar a ciertas preguntas básicas: ¿Qué información se registra? ¿Sobre quién? ¿Por cuánto tiempo? ¿Cuándo se registra la información? ¿Cómo se gestiona la información de otros nodos? ¿Cómo se integra en el registro particular? ¿Cómo se intercambia la información? ¿Cómo asegurar la identidad de un nodo? ¿Cómo se aísla a los nodos? De acuerdo a estas cuestiones, las técnicas propuestas en la literatura deben por lo general especificar los siguientes aspectos:

- Una técnica para la observación del comportamiento de otros nodos. Se debe establecer algún procedimiento para poder observar el comportamiento de los nodos vecinos, y obtener información para poder elaborar tablas donde se resuman las características de este comportamiento y un índice que represente la fiabilidad de los nodos en un solo parámetro denominado reputación.
- Tablas de reputación que reflejen tanto la reputación de los nodos con los que se establece contacto, como otros parámetros que permiten su cálculo, como el porcentaje de paquetes de datos o de señalización retransmitidos, recomendaciones, niveles directos e indirectos de reputación, etc.
- Técnicas para la determinación de un valor de reputación para cada uno de los nodos en función de la información sobre su comportamiento. Se deben especificar tanto el rango de valores que puede adoptar el parámetro de reputación, como la manera de calcularlo a partir de las observaciones realizadas y una interpretación de su significado (qué valores de reputación corresponden a un nodo cooperativo o egoísta).
- Técnicas de recomendación para el intercambio de información sobre reputación de terceros entre los nodos. Las técnicas de recomendación pueden ayudar a acelerar y refinar el proceso de detección de los nodos, así como a hacer efectivo

el aislamiento de los que sean detectados, ya que la identidad de los nodos egoístas identificados se propaga más rápidamente por la red. Sin embargo no se incluye en todas las técnicas de reputación ya que no están exentas de inconvenientes. Por un lado se puede generar un incremento excesivo de la sobrecarga de señalización. Por otro, nodos maliciosos pueden propagar mensajes de acusación falsos.

- Fórmulas y técnicas para la valoración de la fiabilidad de una ruta en función de la reputación de los nodos que lo compongan. Puede consistir simplemente en un promedio de las reputaciones de los nodos implicados. Este valor puede usarse como métrica a la hora de valorar la selección de una ruta por parte del protocolo de enrutamiento.
- Distintos valores umbral. Las técnicas de reputación suelen ser técnicas heurísticas que necesitan valores umbral con los cuales se comparan ciertos parámetros para determinar si se cumplen las condiciones para pasar de un estado a otro en el flujo de la técnica. Entre los más característicos están el umbral de reputación para considerar egoísta o cooperativo un nodo, umbral para considerar segura una ruta, umbral de número de faltas permitidas antes de reducir la reputación de un nodo, reputación de nodos que aparecen por primera vez en las tablas de enrutamiento y de los que no se tiene información previa sobre su comportamiento, etc.
- Distintos valores de temporización: tiempo máximo de vigilancia de un nodo para que retransmita un paquete, tiempo de mantenimiento de reputación antes de devolverla a un valor neutral, tiempo máximo de aislamiento como castigo a un nodo egoísta detectado, etc.

2.3.1 Revisión de técnicas de reputación

A continuación se presentan algunas propuestas de técnicas de incentivo a cooperación en MANETs basadas en reputación. En concreto, la sección analiza sus características, funcionamiento, y principales inconvenientes. Dos de estas técnicas serán comentadas extensamente en las secciones 5.3 y 5.4. Se pueden encontrar excelentes revisiones de los principales trabajos sobre técnicas de reputación en [110] y [44].

Marti [40] inició el campo de las técnicas de incentivo a cooperación basadas en reputación con su técnica basada en dos extensiones ejecutadas por encima del protocolo

de enrutamiento DSR: *watchdog* y *pathrater*[9]. *Watchdog* es una técnica de vigilancia que permite observar si los paquetes enviados para su retransmisión son realmente retransmitidos o no por los siguientes nodos en la ruta. En *watchdog*, la MAC vigila de manera promiscua las transmisiones del nodo que debe retransmitir el paquete en el siguiente salto, para comprobar que la realiza correctamente dentro de un tiempo establecido. En el modo normal de la MAC, un nodo escucha todos los paquetes que capta en su rango, pero sólo pasan hacia las capas superiores aquellos que van dirigidos a él mismo o son difundidos en *broadcast*. En el modo promiscuo de la MAC en cambio, los nodos capturan todos los paquetes que pueden ser escuchados dentro de su rango, y no sólo aquellos que van dirigidos hacia él. En caso de que el nodo vecino no retransmita a tiempo, o bien la retransmisión no sea captada, el nodo que lo vigila incrementa el registro de faltas de ese vecino. Cada nodo lleva un registro de las faltas observadas de aquellos nodos con los que ha interaccionado. El *watchdog* permite de manera sencilla vigilar el comportamiento de los nodos con los que se interactúa. Cuando la cuenta del número de faltas supera cierto umbral, dicho nodo es tachado como egoísta[10], de lo cual es informado el *pathrater* para que el nodo sea evitado en todo establecimiento de ruta posterior emprendido por el protocolo de enrutamiento correspondiente.

El *pathrater* utiliza la información facilitada por *watchdog* para mantener una tabla de reputación de todos los nodos vecinos con los que se establece algún contacto, en la cual se asigna una puntuación a cada nodo en función de su participación o no en el enrutamiento de los paquetes del nodo. Posteriormente, para seleccionar una ruta entre varias alternativas, se escogerá aquella que obtenga un mayor promedio de reputación de sus nodos, o sea, la que a priori sea la más confiable. Además, las rutas usadas durante cierto tiempo, son periódicamente premiadas con un incremento en la reputación de sus nodos.

Lo que las técnicas de *watchdog* y *pathrater* de Marti [40] persiguen es emplear rutas que estén libres de nodos egoístas y también de otros efectos negativos tales como la presencia de nodos congestionados, maliciosos o rutas con enlaces caídos. De esta manera, se mejora el *throughput* al evitar aquellas rutas con menor confiabilidad. Sin embargo, su principal inconveniente es que realmente no consigue incentivar la cooperación de los nodos, ya que no castiga a los nodos egoístas de ninguna manera. Esto hace que sea incluso beneficioso ser egoísta, ya que ningún nodo utilizará a los nodos egoístas para realizar retransmisiones, y de esta manera éstos conseguirán ahorrar energía sin recibir ningún castigo por su egoísmo. [40] también señala casos en los cuales no

[9] Se incluye aquí una breve descripción de la técnica de Marti y *watchdog*, puesto que su descripción detallada se incluye posteriormente en el capítulo 5.

[10] Las condiciones que deben cumplirse para catalogar a un nodo como egoísta varían en las distintas técnicas de reputación. El capítulo 7 estará dedicado al estudio de las técnicas de detección de nodos egoístas.

funciona correctamente la escucha en modo promiscuo de *watchdog*, debido a errores de transmisión radio y colisiones de paquetes que pueden dar lugar a que la técnica confunda una acción cooperativa (retransmisión de paquete) con una acción egoísta. La movilidad de los nodos puede incrementar este fenómeno al hacer que nodos vecinos dejen de estar dentro del rango en instantes posteriores [134]. Al acumularse estos errores, se puede llegar a acusar injustamente de egoísta a un nodo cooperativo.

Por otro lado, el efecto de la movilidad de los nodos y de la detección local de los nodos egoístas es una desventaja que afecta a la mayoría de técnicas de reputación distribuidas. La identidad de un nodo egoísta que ha sido detectado, únicamente es conocida por sus vecinos o por el nodo que haya interaccionado directamente con él. Ese nodo podrá librarse de ser aislado si establece rutas con nodos que no conozcan su identidad, lo cual se ve además facilitado por la movilidad de los nodos. Difundir la identidad de los nodos egoístas es notablemente difícil en sistemas distribuidos. Ambos inconvenientes serán tratados a lo largo de la tesis. [121] prueba que los nodos de una red MANET son capaces de llegar a converger a unos niveles comunes de reputación mediante un sistema de intercambio local de esos niveles entre los nodos. Sin embargo, una velocidad de convergencia demasiado lenta frente al dinamismo de la red y la carga de señalización que implica el intercambio local de recomendaciones pueden ser inconvenientes a este sistema distribuido.

Watchdog es la técnica de observación más aceptada en las técnicas de reputación evaluadas. Sin embargo, debido a sus inconvenientes, algunos trabajos han propuesto distintas mejoras para el *watchdog* básico de Marti [40]. [50] y [125] proponen mejorar las prestaciones del *watchdog* básico mediante un enfoque Bayesiano, más robusto frente a los errores de observación. El *watchdog* Bayesiano es tratado más detalladamente en la sección 2.5 y en el capítulo 7. [63] propone el concepto de *watchdog* colaborativo para hacerlo aún más robusto frente a los errores; el concepto consiste en compartir la información de las observaciones realizadas entre los nodos vecinos.

A pesar de sus inconvenientes, la mayoría de las técnicas de reputación en la literatura utilizan el mecanismo de observación promiscua de *watchdog* para observar el comportamiento de los nodos. A continuación se mencionan algunas de las más destacadas. [111] presenta un mecanismo de inferencia basado en el contexto que permite detectar comportamientos maliciosos en el proceso de enrutamiento. Una vez finalizado el establecimiento de la ruta, también impide que los nodos egoístas diseminen informes falsos de caídas de enlaces para evitar la retransmisión de paquetes. El nodo origen de una transmisión recibe mensajes especiales de acusación SECM (*SECurity Message*) por parte de otros nodos que detectan algún nodo egoísta en la ruta. Un nodo no puede ser culpabilizado hasta que el nodo origen haya recibido por lo menos tres acusaciones de tres vecinos diferentes, para evitar acusaciones falsas. [112] presenta CONFIDANT

(*Cooperation Of Nodes: Fairness In Dynamic Ad-hoc. NeTworks*), otra técnica de reputación basada en cuatro módulos: monitorización, gestión de confianza, sistema de reputación, y gestión de rutas. El módulo de monitorización funciona de manera similar a la técnica *watchdog*, si bien no sólo escucha en modo promiscuo la retransmisión de los vecinos sino que controla el comportamiento del protocolo de enrutamiento. Si un nodo detecta algún comportamiento anómalo, envía mensajes de aviso ALARM a todos sus nodos amigos. Estos nodos determinan la confianza del mensaje según el nivel de confianza del remitente. A partir de esta información, el sistema de reputación mantiene una lista de confianza y una lista negra en cada nodo, e intercambia esta lista con sus amigos. La lista negra contiene todos aquellos nodos que deben ser evitados a la hora de establecer rutas, mientras que la lista de confianza contiene la confianza de cada nodo. Además, cada nodo también evita enrutar las peticiones que provienen de los nodos de la lista negra, marcando una diferencia importante con el sistema *watchdog* que únicamente evitaba a los nodos egoístas pero no los aislaba. El módulo de gestión de rutas actúa de manera similar al *pathrater* de Marti. Sin embargo, de manera similar al *watchdog*, no puede distinguir con seguridad un comportamiento malicioso de una simple colisión. Además también puede tener problemas de escalabilidad en los aspectos de validación de clave y certificación por parte del módulo de gestión de confianza.

CORE [82] incentiva la cooperación con una técnica colaborativa de monitorización, ya que utliza informes positivos propagados por nodos vecinos (denominado en [82] reputación indirecta) además de sus propias observaciones (reputación directa). Además, cada nodo vigila la correcta realización de funciones concretas de enrutamiento (reputación funcional) como retransmisión de paquetes de enrutamiento, de paquetes de datos, etc… Estos tres tipos de reputación se utilizan para calcular una reputación combinada. Cuando dicha reputación cae por debajo de cierto valor, el nodo es aislado de la red. De todas maneras, los nodos aislados pueden volver a unirse a la MANET si cooperan adecuadamente una vez transcurrido cierto tiempo de castigo. Con esta técnica se evitan las falsas acusaciones por parte de nodos maliciosos, ya que no pueden difundir informes negativos, sólo positivos. Además, se utiliza un factor temporal corrector para calcular la reputación combinada que da más peso a las observaciones pasadas que a las actuales, con la intención de evitar falsos positivos provocados por malas condiciones del canal radio, congestión o colisiones. TEAM [47] sigue la filosofía de CORE [82] en el sentido de utilizar varios tipos de reputación (directa, indirecta y recomendada[11]) y combinarlos para hallar la reputación de cada nodo. Sin embargo, introduce algunas novedades notables, como la de que las recomendaciones se deduzcan de manera implícita a partir de los mensajes que recibe cada nodo que participa en la transmisión

[11] En este caso, la terminología referente a los tipos de reputación sí sigue el convenio adoptado en este trabajo, explicado en la nota 8.

multi-salto de un paquete. De esta manera se consiguen dos objetivos: evitar la sobrecarga de señalización de las recomendaciones convencionales y aumentar la fiabilidad de las recomendaciones. Esta será una de las técnicas de referencia utilizadas a lo largo de la tesis, y se detallará su funcionamiento en la sección 5.4.

Mientras que CORE [82] intenta evitar los problemas de baja fiabilidad del canal radio dando un mayor peso a las observaciones pasadas frente a las observaciones actuales, en [114], los autores proponen justo lo contrario para incentivar a los nodos a colaborar continuamente sin darles ocasión a acumular una buena reputación que les permita dejar de hacerlo temporalmente. Sin embargo, esta política permite que un nodo que se ha comportado egoístamente pueda recuperar rápidamente una buena reputación.

Característica	Referencia
Uso de *watchdog*	[40][47][82][15]
Mejora del *watchdog*	[50][63][112][133][134]
Alternativas al *watchdog*	[111][128][129][130][131][132][49]
Uso de confirmaciones	[128][129][130][131][132]
Promedio de reputación para selección de rutas	[40][82]
Mensajes de alarma	[112]
Posibilidad de redención	[82]
Vigilancia de funciones específicas	[82]
Promedio de distintos tipos reputación	[82][47]
Filtro temporal de observaciones antiguas	[114][50][134][49]
Filtro temporal de observaciones recientes	[82]
Listas públicas de identidad de egoístas	[120]
Recomendación explícita	[121][82][117][118][119]
Reputación recomendada implícita	[49]
Considerar sesgo del nodo que recomienda	[49] [119]
Considerar antigüedad de nodos	[120]
Considerar semejanza entre recomendación y creencia previa	[121]

Tabla 2-5. Técnicas de incentivo a cooperación basadas en reputación.

Por otro lado, la técnica *watchdog* propuesta por Marti no es la única técnica de observación empleada en la literatura. Otros trabajos proponen técnicas de observación alternativas que pueden usarse en sustitución del *watchdog*. Algunos trabajos ([128], [129], [130], [131] y [132]) proponen que los nodos que reciban los paquetes

correctamente envíen mensajes de confirmación a los nodos que los transmiten para que tengan constancia que los nodos intermedios los han retransmitido correctamente. En concreto, [128] propone que cada nodo envíe un mensaje ACK (*ACKnowledgment*) al nodo situado dos saltos atrás. Sin embargo, introducen una considerable sobrecarga de señalización. [133] utiliza una combinación de la técnica *watchdog* y mensajes de confirmación. [49] propone evaluar datos estadísticos extraídos de las observaciones de los nodos para predecir el comportamiento del nodo. La Tabla 2-5 muestra un resumen de las principales técnicas de incentivo a cooperación basadas en reputación discutidas en esta sección.

En [115] se señalan algunos de los inconvenientes de las técnicas de reputación:

- En primer lugar, la reputación no es un valor fácil de determinar a partir de las observaciones, principalmente por los problemas ya mencionados inherentes al método de observación *watchdog*, pero también porque algunas de las acciones de un nodo que siguen estos sistemas, como aislar a nodos egoístas, puede parecer un comportamiento egoísta a los ojos de otros nodos que no conozcan el egoísmo del nodo aislado [113]. [120] propone que cada nodo publique periódicamente en modo *broadcast* una lista con las identidades de tres tipos de nodos: aquellos a los que presta servicio (amigos), aquellos a los que no presta servicio (enemigos), y aquellos que no han prestado servicio al nodo (egoístas), lo cual puede evitar el problema pero tiene un excesivo coste en términos de sobrecarga de señalización.
- En segundo lugar, como se comentaba en el párrafo anterior, distribuir consistentemente la información de reputación necesaria incurre en un alto coste en términos de sobrecarga de señalización, siendo especialmente problemático para redes MANETs medianas o grandes. Además, no se puede garantizar la confiabilidad de los mensajes de información de reputación debido a la existencia de nodos maliciosos que incluso pueden aliarse entre sí propagando información falsa. [117] propone evitar las falsas acusaciones en las recomendaciones de reputación utilizando la propia reputación de los nodos que recomiendan a otros nodos para valorar la fiabilidad de la recomendación que realizan. [118] introduce el concepto de madurez para dar más importancia a las opiniones de los nodos con los que lleva más tiempo intercambiando opiniones. En [119], se compara la opinión sobre reputación que los demás nodos propagan con la reputación que el nodo guarda en sus tablas. Si ambos niveles de reputación son

muy distintos, se rebaja la confiabilidad[12] del nodo que ha realizado la recomendación. En caso contrario, se tiene en cuenta su recomendación.

- En tercer lugar, todos los sistemas de reputación son en general vulnerables a un ataque en el que el nodo egoísta cambia continuamente su identidad, bien entrando y saliendo de la red o bien porque debido a la movilidad, los nodos vecinos cambian continuamente y no están al tanto del egoísmo de los nuevos vecinos. La movilidad también afecta al mantenimiento de los enlaces y al funcionamiento del *watchdog*, ya que un nodo puede ser acusado de egoísta cuando en realidad lo que puede haber ocurrido es que el enlace se haya roto por la movilidad de algún nodo intermedio. Este y otros efectos indeseables comentados hacen que sea necesario evaluar las prestaciones de la técnica *watchdog* en condiciones realistas de simulación.
- Por último, algunas técnicas como CORE [82] especifican que un nodo aislado puede reintegrarse si se observa un buen comportamiento durante un período de tiempo, pero parece obviar el problema de que si un nodo permanece aislado, no podrá interaccionar con otros nodos y por tanto, aunque lo quiera, no podrá demostrar un buen comportamiento. La publicación de listas con la identidad de aquellos nodos a los que no se da servicio por parte de los nodos en [120] ayuda a contrarrestrar este efecto. [116] propone paliar los inconvenientes de las técnicas de reputación utilizando información de redes sociales de los usuarios de los nodos.

2.4 Dimensionamiento y viabilidad de técnicas basadas en reputación

La mayoría de los trabajos sobre técnicas de incentivo a cooperación en redes MANET suelen recurrir a simulaciones para evaluar y validar las técnicas propuestas. Sin embargo, en muchos casos se observó que las condiciones de simulación en las que se llevaron a cabo podrían ser poco realistas, y por tanto inducir a conclusiones erróneas. El riesgo principal en que se incurre al asumir unas condiciones poco realistas es el de infravalorar el error que aparece al observar el comportamiento de los nodos. La mayoría de las técnicas de reputación utilizan la técnica *watchdog* para observar el comportamiento de los nodos vecinos. Como se comentó anteriormente, la técnica *watchdog* tiene algunos inconvenientes derivados de las características de las comunicaciones en el canal radio, que incluyen errores de transmisión y colisiones de

[12] La confiabilidad de un nodo se aplica al grado de fiabilidad que tienen las recomendaciones de ese nodo.

paquetes que conllevan a errores en la observación. Como se verá, los errores de observación pueden provocar que nodos que realizan las retransmisiones correctamente, sean acusados erróneamente de estar descartando paquetes. La capacidad de detección de las técnicas de reputación es uno de los factores que mayor influencia puede tener en el rendimiento de las mismas, y por tanto debe ser estudiado con la mayor precisión. Esto exige evaluar su rendimiento considerando un grado de realismo adecuado en el modelo del canal radio, que tenga en cuenta no sólo el efecto más básico de la pérdida de señal por propagación con la distancia, sino también otros como la posible presencia de obstáculos que impidan la visibilidad directa tales como edificios, la correlación espacial del desvanecimiento lento y el desvanecimiento rápido.

Ref.	Modelo canal / rango [m]	Tamaño [m^2]	Número nodos	Movilidad
[40]	Propagación básica	670x670	50	Random waypoint
[64] [65]	Propagación básica / 120	500x500	100	Random waypoint
[121]	Propagación básica / 30	400x400	20 - 100	Random waypoint
[112]	Propagación básica / 250	1000x1000	50	Random waypoint
[41]	Propagación básica / 250	670x670	40	Random waypoint
[122]	Propagación básica / 250	1500x1000	50	Random waypoint
[123]	Propagación básica / 250	Circular radio 200 m	3 – 22	Topología en anillo
[124]	Propagación básica / 150	600x600	50 – 300	Random waypoint
[125]	Propagación básica	1500x1000	50	Random waypoint
[71]	Propagación básica / 250	1000x1000	50	Random waypoint
[126]	Propagación básica / 377	2000x600	100	Random waypoint
[47]	Propagación básica	1200x1200	100	Random waypoint
[127]	Propagación básica / 250	1500x1000	27	Random waypoint
[68]	Propagación básica / 100	500x500	100	Random waypoint
[53]	Propagación básica / 250	1000x1000	25 - 200	Random waypoint
[33]	Propagación básica / 100	1000x1000	100 - 900	Semi-Markov Smooth SMS [137]
[50]	Propagación básica / 250	1000x1000	10 - 50	Random waypoint
[118]	Propagación básica / 250	150x150	4	Ad-hoc (peor caso)
[63]	-	1000x1000	50	Random waypoint

Tabla 2-6. Valores de parámetros de simulación de técnicas de incentivo a cooperación.

La Tabla 2-6 muestra las condiciones de simulación asumidas en una colección de los trabajos de incentivo a la cooperación presentados a lo largo del capítulo. Puede

observarse que en todos ellos se asume el modelo de canal más sencillo, de pérdidas básicas de propagación. En este modelo, se establece un rango de distancia dentro del cual se supone que la comunicación se realiza con éxito, mientras que fuera de ese rango, los nodos no pueden comunicarse entre sí. Este modelo sólo tiene en cuenta por tanto las pérdidas por propagación con la distancia. Como se verá en los capítulos siguientes, el modelo de propagación básica es insuficiente a la hora de evaluar con precisión el rendimiento de las técnicas de incentivo a cooperación. Las únicas diferencias en la Tabla 2-6 en cuanto al modelo de canal corresponden al rango asumido, que debe ajustarse para conseguir una conectividad aceptable, junto con el número de nodos y la dimensión total del escenario, parámetros que también se muestran en la Tabla 2-6. Sin embargo, ajustar correctamente estos parámetros no es suficiente para conseguir una precisión adecuada en la simulación del proceso de transmisión de paquetes en el canal radio, y esto hace que se infravalore los errores de observación de la técnica *watchdog*. Este será por tanto el cometido del capítulo 5, en el que se evalúa el rendimiento de dos técnicas de reputación de la literatura, considerando diferentes niveles de realismo en la simulación, y comparando los resultados obtenidos. De esta manera se constata la necesidad de utilizar unas condiciones de simulación suficientemente realistas. Asimismo, este análisis muestra que en trabajos anteriores se había sobrestimado la capacidad de *watchdog* para observar adecuadamente las acciones egoístas de los nodos. Al evaluar en condiciones realistas su rendimiento, muchos nodos cooperativos son acusados incorrectamente, y por tanto el objetivo del capítulo 6 es proponer y evaluar técnicas que ayuden a limitar las acusaciones incorrectas.

2.5 Técnicas de detección

Como se comentó en el apartado anterior, las técnicas de reputación suelen tener dos módulos bien diferenciados, si bien algunas propuestas particulares proponen otras estructuras más compartimentadas [112]. La Figura 2-1 muestra un diagrama con los módulos principales de las técnicas de reputación. El módulo de monitorización observa y registra el comportamiento de los nodos vecinos mientras que el de reacción debe emprender acciones en función de las observaciones realizadas por el módulo de monitorización. Estas acciones, ejecutadas con la ayuda del protocolo de enrutamiento empleado, pueden consistir en seleccionar las rutas para los paquetes y aislar o no a un vecino así como retransmitir o no las peticiones de enrutamiento entrantes. En el interfaz entre ambos módulos, se sitúan las técnicas de detección. Su misión es evaluar el registro de observaciones de un nodo y determinar si debe ser acusado de comportarse egoístamente y desencadenar el consecuente proceso en el módulo de reacción. Esta evaluación no necesita hacerse periódica ni continuamente, sino únicamente tras cada

nueva observación realizada y registrada por el módulo de monitorización. El objetivo de las técnicas de detección es realizar las decisiones de acusación minimizando los dos posibles tipos de error: por acusación incorrecta (de un nodo cooperativo), o por no acusación incorrecta (de un nodo egoísta), también denominados falso positivo y falso negativo, respectivamente. El error cometido al realizar la decisión de acusación proviene de la incertidumbre que introduce el canal radio. Como se ha comentado, esta incertidumbre provoca que algunas de las observaciones realizadas sean incorrectas y por tanto conduzcan a decisiones erróneas. Además, otro factor a tener en cuenta es el retardo en la detección, es decir, cuántas observaciones son necesarias antes de tomar la decisión de acusar a un nodo. Los retardos elevados favorecen que el nodo descarte paquetes en caso de que sea un nodo egoísta. Sin embargo, en el diseño de las técnicas de detección debe tenerse en cuenta que existe un compromiso entre los tres factores mencionados: los dos tipos de error y el retardo de detección [138]. Un buen diseño debe tratar de optimizarlos a la vez y hallar un equilibrio entre ellos. Este será el objetivo del capítulo 7.

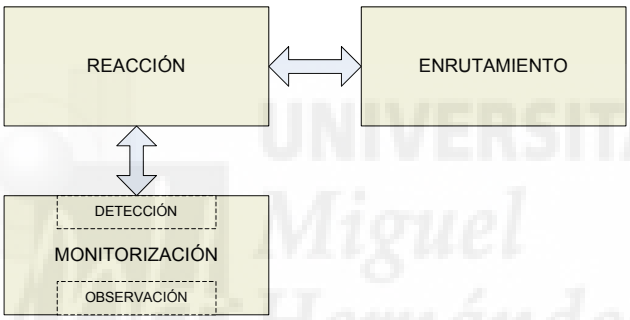


Figura 2-1. Diagrama general de técnicas de reputación.

En trabajos anteriores se han propuesto técnicas de detección bayesianas que tratan de fortalecer el *watchdog* estándar frente a los errores introducidos por transmisión radio en el canal. Los trabajos sobre detección bayesiana emplean distintas variaciones heurísticas con una misma filosofía, que se expone y formaliza en el trabajo [50]. En su versión más simple, el *watchdog* Bayesiano consiste en registrar el número de observaciones de comportamientos egoístas de un nodo y el número de observaciones totales. El grado de egoísmo del nodo se mide como el cociente entre ambos números. Cuando el cociente supera cierto umbral, el nodo es acusado de comportarse egoístamente. Sin embargo, debido a la naturaleza del canal radio, algunas de las observaciones de comportamiento egoísta podrían ser en realidad achacables a colisiones de paquetes o errores de transmisión, y por tanto el umbral de acusación escogido debe tener en cuenta la probabilidad de error en la observación. Esto supone un compromiso entre los dos posibles tipos de error comentados: acusación incorrecta y no acusación incorrecta. Dado que la elección de un valor para el umbral de acusación debe tener en cuenta este compromiso además de las condiciones de simulación y las características del canal radio

simulado, la mayoría de los trabajos de investigación evaluados suelen omitir la especificación de un valor concreto.

[50] propone algunas variaciones del *watchdog* Bayesiano, como son introducir un factor de envejecimiento o de atenuación, que otorga una mayor importancia a las observaciones recientes frente a las observaciones antiguas, de manera que el nodo debe permanecer siempre atento a retransmitir correctamente, puesto que será más difícil acumular una buena reputación al ir desvaneciéndose la reputación alcanzada en el pasado. En este punto, es interesante remarcar que no existe acuerdo en cuanto a si al aplicar una ponderación temporal a las observaciones, es más beneficioso dar más importancia a las observaciones más recientes como hace [50], o si por el contrario es mejor valorar más las observaciones más antiguas como propone [53]. [49] introduce otra variación similar en el *watchdog* Bayesiano, que consiste en establecer una ventana temporal de k observaciones. Sólo se tienen en cuenta las últimas k observaciones, despreciando las anteriores. [38] y [48] también adoptan el enfoque Bayesiano del *watchdog* en sus propuestas. [134] implementa y evalúa el rendimiento de un *watchdog* Bayesiano con envejecimiento para fortalecer la seguridad de una red inalámbrica que provee de acceso a Internet a un área rural. [63] propone el concepto de *watchdog* bayesiano colaborativo, que consiste en compartir la información de las observaciones realizadas entre los nodos vecinos para mejorar las prestaciones del *watchdog* bayesiano individual. De esta manera, los nodos compilan mayor información sobre los nodos vecinos comunes, a través del intercambio de mensajes con nodos vecinos. De esta manera, al tener mayor cantidad de información, se reduce el error introducido por el canal de transmisión y por las eventuales colisiones de paquetes.

La Tabla 2-7 recopila las características de diferentes tipos de técnicas de detección basadas en *watchdog* que además utilizan el enfoque bayesiano para mitigar los errores de observación.

Tipo de *watchdog*	Referencias
Watchdog estándar	[40]
Bayesiano estándar	[50] [38] [48]
Bayesiano con envejecimiento	[50] [134]
Bayesiano con ventana temporal	[49]
Bayesiano colaborativo	[63]

Tabla 2-7. Técnicas de observación de comportamiento basadas en *watchdog*.

2.6 Técnicas de reputación con asistencia centralizada

A pesar de que una de las características más favorables de las técnicas de incentivo basadas en reputación era que permitían no alterar el carácter distribuido de los protocolos de las redes MANET, algunos investigadores han estudiado la posibilidad de solucionar algunos de los problemas de las técnicas de reputación empleando algún tipo de entidad central de control que las asistiera en ciertas funciones. En este contexto, uno de los primeros trabajos que propuso aprovechar la infraestructura de las redes celulares para ayudar en la señalización y el control de redes MANET fue [135]. En dicho trabajo, se propone una arquitectura denominada CAHN (*Cellular Assisted Heterogeneous Networking*) que, aprovechando la infraestructura de las redes celulares, gestiona de manera eficiente las comunicaciones en redes híbridas formadas por sistemas celulares y redes MANET. Algunas características de las redes de comunicaciones celulares, hacen que su utilización para asistir en tareas de gestión de redes MANET sea especialmente provechosa. Entre estas tareas se encuentra la autenticación de la identidad de los nodos, el enrutamiento, control de acceso, etc. Si bien podría objetarse que en cierta manera con este sistema se pierde el requisito de red distribuida de las redes MANET convencionales, las ventajas que se obtienen en estas redes híbridas superan este inconveniente. Además, la ubicuidad de las redes celulares contribuye a que la aplicación de esta filosofía sea transparente para el usuario.

[102] propone la incorporación de unos agentes denominados "*CAMA agents*" a la red celular que gestionan la información de control de una red MANET formada dentro del área de cobertura de la red. La información de enrutamiento y seguridad de la red MANET se transmite a través de canales radio de la red celular. Otros trabajos [136] insisten en la idea de redes híbridas tipo MCN con retransmisores móviles, en las que los usuarios con mejores condiciones del enlace radio hacia la estación base hacen de proxy para otros. [136] propone además la utilización de una técnica basada en créditos para incentivar la cooperación de los nodos en la retransmisión de los paquetes. De esta manera, la utilización de la infraestructura celular soluciona alguno de los inconvenientes de las técnicas de incentivo basadas en crédito, como la necesidad de una entidad central confiable.

Finalmente, [53] centra su atención en mejorar la seguridad y combatir el egoísmo de los nodos en redes MANET. Propone utilizar redes inalámbricas de área extensa como son las redes celulares para solventar el problema de la identidad de los nodos en la red MANET. De esta manera, los nodos serían autenticados por una entidad de la red celular denominada servidor central, de un modo similar a como ya se propuso en [135]. Además, se establece una técnica heurística de reputación que utiliza la técnica *watchdog* como sistema de monitorización del comportamiento de los nodos vecinos a nivel local.

Cuando algún nodo detecta que la reputación de un nodo vecino es inferior a cierto umbral, informa al servidor central, que evalúa si la acusación proviene o no de un nodo confiable. Se tiene en cuenta además que un número suficiente de acusaciones provenientes de diferentes nodos poco confiables equivalen a una acusación de un nodo completamente confiable. Los nodos acusados son aislados, pero pueden optar a volver a recuperar su reputación a cambio de retransmitir un cierto número de paquetes para otros nodos. Sin embargo, no parece encarar el problema de que las acusaciones incorrectas no vienen sólo de que nodos maliciosos intenten propagar acusaciones inventadas intencionadamente. Como se comprobará a lo largo de la tesis, la mayoría de las acusaciones erróneas provienen del error en la técnica de observación *watchdog* introducido por errores de transmisión y colisiones de paquetes en el canal radio, y por tanto, son no intencionadas. Por ello, se hace necesario emplear técnicas para paliar las acusaciones incorrectas, y reducirlas al máximo, y con más razón cuando se considera como en este caso un aislamiento global de los nodos acusados[13]. Tampoco se proporciona ningún valor de los parámetros de configuración de la técnica de detección heurística que aplican para acusar a los nodos egoístas. Por último, las condiciones de simulación consideradas son, como en la mayoría de los trabajos de reputación, poco realistas, especialmente en cuanto al modelo de canal escogido[14], y por tanto no permiten apreciar el problema de las acusaciones incorrectas en su correcta dimensión.

La Tabla 2-8 muestra un resumen de las características principales de las técnicas de reputación centralizadas que se han mencionado en esta sección.

Características	Referencias
Control de acceso y gestión identidad	[135][53]
Gestión de redes híbridas	[135]
Gestión de enrutamiento	[102]
Gestión de seguridad	[102]
Control centralizado de reputación	[53]
Alarmas locales por egoísmo	[53]

Tabla 2-8. Técnicas de incentivo a cooperación centralizadas basadas en reputación.

[13] Los nodos que sean acusados de comportarse egoístamente, serán aislados a nivel de toda la red MANET, ya que la información sobre su egoísmo estará disponible para todos los nodos de la red. Por ello deben reducirse al máximo las acusaciones incorrectas.

[14] [53] supone un modelo de canal de propagación básico, con un alcance de 250 metros, como puede apreciarse en la Tabla 2-6.

2.7 Resumen

El presente capítulo ha descrito el estado del arte en cuanto a técnicas de incentivo a cooperación, haciendo especial hincapié en las técnicas de reputación en redes MANET. Al inicio del capítulo se mencionaron las características de las redes MANET, concretamente el hecho de que las funciones de la red deben ser realizadas de manera distribuida por los mismos nodos. Esto implica que los nodos deben seguir fielmente los protocolos establecidos para la comunicación, o de lo contrario la existencia y el funcionamiento de la red pueden verse comprometidos. Sin embargo, por distintos motivos, los nodos pueden escoger no realizar alguna de estas funciones, en lo que se ha denominado comportamiento no cooperativo de los nodos. Se discutieron los tipos de comportamiento no cooperativo y los ataques contra la seguridad y la integridad de la red y de los datos de los usuarios. La clasificación más general incluía las siguientes categorías de comportamientos no cooperativos: nodos egoístas, nodos maliciosos, nodos inactivos y nodos desconectados. Los nodos egoístas se caracterizan porque la motivación para no cooperar no es la de perjudicar al funcionamiento de la red, sino la de preservar su propia batería u obtener algún tipo de ventaja similar sobre el resto de los nodos de la red. Dentro de los nodos egoístas también caben distintas subcategorías dependiendo de si se descartan todos los paquetes, o solo una parte según una cierta probabilidad p, o según el nivel de batería restante. También se han mencionado los efectos que el egoísmo de los nodos puede causar en la red, entre los que cabe citar una reducción de la conectividad, que puede llevar a la segmentación de la red, el aumento del número de saltos y de la energía empleada por los nodos en retransmitir los paquetes, reducción de la velocidad de transmisión, etc. haciendo inviable la comunicación cuando la proporción de nodos egoístas es demasiado alta.

A continuación, el capítulo analiza las distintas categorías de técnicas de incentivo a cooperación que han sido propuestas en la literatura, que incluyen las técnicas basadas en crédito, las técnicas basadas en teoría de juegos y las técnicas basadas en reputación. Una cuarta categoría engloba a las técnicas que no se pueden incluir en el resto, que suelen combinar alguna de las otras categorías. Las técnicas basadas en crédito constituyen una solución semejante a la prestación de servicios en la vida real a cambio de una remuneración económica. Sin embargo, adolecen de algunos inconvenientes como la necesidad de una entidad central o de un módulo hardware a prueba de manipulaciones, entre otros. Por otro lado, la teoría de juegos ha demostrado una gran capacidad para analizar el comportamiento de los nodos y las posibles estrategias de equilibrio frente al egoísmo en redes MANET. Algunos estudios han investigado si realmente es necesario incentivar a los nodos a cooperar, y bajo qué condiciones comportarse egoístamente es la opción más racional. Sin embargo, la mayoría de estos estudios deben realizar

simplificaciones poco realistas, y por ello las conclusiones obtenidas pueden no ser válidas en situaciones reales.

En el capítulo, se han discutido también las técnicas basadas en reputación, las cuales tratan de detectar a los nodos egoístas y de propagar su identidad para aislarlos y que no sean utilizados ni como retransmisores ni como origen o destino de flujos de datos. El propósito que persigue el aislamiento de los nodos egoístas es evitar que descarten los paquetes que deben retransmitir e incentivarlos a cooperar. La mayoría de técnicas basadas en reputación utiliza como método de observación la técnica *watchdog*, que consiste en poner la MAC del terminal en modo promiscuo para que sea capaz de observar si el nodo siguiente en el flujo de datos retransmite correctamente o no el paquete que debe retransmitir en un tiempo establecido. A pesar de la facilidad de aplicación del *watchdog*, el canal radio introduce un cierto error de observación que proviene de potenciales errores de transmisión y de colisiones de paquetes, que aumentan el número de acusaciones incorrectas. Por ello algunos estudios han propuesto refinamientos del *watchdog* original (*watchdogs* bayesianos, colaborativos, etc.) para robustecerlo frente al error introducido por el canal radio. Otros estudios proponen técnicas alternativas al *watchdog*, basadas principalmente en confirmaciones explícitas, o bien en control de flujo de paquetes extremo a extremo. Las técnicas de reputación se han ido refinando al introducir conceptos como los de reputación directa, indirecta y recomendada, mejorando los procesos de intercambio de mensajes de recomendación, etc.

A pesar de las mejoras introducidas, se ha detectado que los estudios evaluados empleaban unas condiciones de simulación poco realistas. En concreto, el modelo de canal adoptado en casi todos ellos (modelo de propagación básica con un rango de transmisión fijo) no reproduce adecuadamente los fenómenos del canal radio que pueden afectar al funcionamiento del *watchdog*. Por ello, el primer capítulo de resultados de esta tesis (el capítulo 5) aborda el dimensionamiento de las condiciones y los procedimientos apropiados para la evaluación realista de las técnicas de reputación en una red MANET con presencia de nodos egoístas.

Por otro lado, como se ha comentado, las técnicas de detección bayesianas basadas en el *watchdog* tienen como objetivo robustecer el *watchdog* original para hacerlo menos sensible a los errores introducidos por la transmisión en el canal radio, y por tanto menos propenso a generar acusaciones incorrectas. Sin embargo, se ha detectado que cuando se quiere optimizar el rendimiento de las técnicas de detección, existe un compromiso entre los distintos parámetros de rendimiento, que son el número de acusaciones incorrectas, el número de no acusaciones incorrectas, y el número de paquetes descartados por los nodos egoístas antes de su detección. Es decir, existe un compromiso entre el retardo y la precisión del proceso de detección, agravado por las condiciones dinámicas y cambiantes del canal radio, que introduce niveles de error variable en distintas situaciones. En este

contexto, uno de los objetivos de la tesis será mejorar las técnicas de detección usadas en las técnicas de reputación. Finalmente, se ha revisado también el estado del arte de aquellas técnicas de reputación que proponen la utilización de una entidad central como asistente a los procesos de detección y aislamiento de los nodos. Este enfoque contribuye a solucionar algunos de los problemas tradicionales de las técnicas de reputación, como autenticar la identidad de los nodos para que no puedan evitar el castigo y un aislamiento más eficaz. Es por ello que en esta tesis también se aplica este enfoque, explotando sus posibilidades más allá de los planteamientos propuestos en trabajos anteriores que han sido detallados en este capítulo. Pero antes de pasar a los capítulos de resultados (capítulos 5 a 8), en los siguientes capítulos se aclararán algunas cuestiones previas que servirán de referencia e introducción al cuerpo principal de la tesis.

3

Redes inalámbricas

Uno de los objetivos de la presente tesis es el diseño y análisis de técnicas de incentivo a la cooperación basadas en reputación en redes celulares multi-salto, que permitan optimizar el rendimiento global de la red incentivando a los nodos a participar en las retransmisiones. Por ello, este capítulo está dedicado a revisar los aspectos de las redes de comunicaciones celulares y de las redes MANET que están más relacionadas con los objetivos de la tesis. Se hace especial hincapié en la tecnología 802.11, y en los aspectos de capa física, nivel de enlace y protocolos de enrutamiento directamente relacionados con la simulación de una red multi-salto. Se presenta el nivel físico y de enlace del estándar 802.11 [3] y el protocolo de enrutamiento usado en las simulaciones de la tesis: DYMO (*DYnamic MANET On-demand routing protocol*) [25], que es una evolución mejorada de AODV[15] [7]. En cuanto a las redes celulares, se hace una breve introducción de su evolución en sucesivas generaciones hasta los sistemas desplegados y en uso comercial actualmente. También se describen las características más novedosas del sistema HSDPA, que es el empleado para los estudios realizados en la presente tesis, respecto al sistema de comunicaciones móviles de la generación anterior, UMTS (*Universal Mobile Telecommunications System*). Se muestran algunos aspectos específicos del interfaz radio de HSDPA, los cuales serán útiles para entender posteriormente el modelo escogido para simular la parte celular de la red MCN en el estudio llevado a cabo en el capítulo 8.

[15] AODV por su parte sirve de base para el protocolo de enrutamiento HWMP (*Hybrid Wireless Mesh Protocol*) [8] utilizado en el sistema 802.11s [5] para redes malladas.

3.1 Redes MANET

En los últimos años, se ha ido incrementando cada vez más el uso de tecnologías inalámbricas en redes locales, gracias a la proliferación de dispositivos electrónicos de comunicaciones con acceso a distintas tecnologías radio, entre las cuales cabe destacar la tecnología WiFi por su enorme aceptación[16]. Esta tecnología pertenece a la categoría de redes inalámbricas de área local o WLAN (*Wireless Local Area Network*). Tienen un rango típico de entre 100 y 500 metros. Funcionan igual que las redes LAN cableadas: alta capacidad, conectividad total entre las estaciones conectadas, y posibilidad de transmisión *broadcast*. Sin embargo, para su aprovechamiento deben tenerse en cuenta aspectos específicos de redes inalámbricas tales como seguridad, consumo de potencia, movilidad, limitación de ancho de banda en el interfaz aire, etc. [9].

Existen dos tipos fundamentales de WLAN: las que se basan en una infraestructura o las puramente ad-hoc o redes MANET (*Mobile Ad-hoc Network*). En el modo infraestructura se requiere la existencia de un controlador central, que generalmente está conectado a la red cableada y proporciona acceso a Internet al resto de dispositivos móviles conectados. Por el contrario, una red MANET consiste en un conjunto de nodos móviles inalámbricos que pueden organizarse a sí mismos de manera dinámica y autónoma en topologías de red temporales, de manera que las personas y los dispositivos de un entorno se puedan interconectar sin necesidad de una infraestructura de comunicación preexistente [9].

El crecimiento del mercado de dispositivos electrónicos de comunicación de bajo coste y orientados hacia aplicaciones civiles (*Bluetooth*, *WiFi*, etc.) ha despertado el interés de los investigadores hacia las redes MANET, más allá de las aplicaciones militares más evidentes. En este escenario, los dispositivos móviles se organizan a sí mismos para crear una red a través de sus interfaces radio, sin necesidad de una infraestructura previa, de manera espontánea, dinámica y con carácter temporal. Esta tecnología ofrece una solución efectiva a distintas necesidades profesionales o de consumo con un rango limitado, que puede extenderse a través de la tecnología multi-salto. Este tipo de redes se denominan redes MANET de propósito general o redes MANET puras, donde el término "puro" se refiere a que el paradigma MANET se sigue de manera estricta: no es necesaria ninguna autoridad ni infraestructura encargada de controlar y gestionar las funciones de red. El término "propósito general" se refiere a que estas redes no están diseñadas para una aplicación específica, sino más bien, que son capaces de soportar cualquier aplicación sobre TCP/IP: transmisión de vídeo [10],

[16] Wifi es el sistema con el que la industria popularizó la familia de estándares 802.11 de redes inalámbricas de área local desarrollado por el IEEE.

telefonía sobre IP [11], aplicaciones de intercambio de ficheros P2P [12], aplicaciones multimedia [13], etc.

Algunos investigadores son críticos en cuanto a los resultados de la investigación sobre redes MANET de propósito general, alegando que no ha conseguido logros notables en términos de implementación en el mundo real [14]. A pesar de ello, la tecnología MANET ha probado su eficiencia cuando ha sido orientada a aplicaciones específicas. Las redes *mesh*[17] o redes de malla constituyen una evolución a corto plazo de las redes multi-salto ad-hoc [5]. Estas redes introducen enrutadores fijos que reducen considerablemente la complejidad del diseño de la red. Con el apoyo de la infraestructura, las redes de malla pueden llevar las redes MANET de propósito general al mercado proporcionando un acceso a Internet flexible y a un bajo coste [15]. Por otro lado, las redes oportunísticas hacen referencia a cierto tipo de red MANET que proporcionan conectividad ubicua en escenarios en los que no se encuentra disponible en todo momento una conexión directa a Internet. Los dispositivos de estas redes, dotados con distintas tecnologías radio, se encuentran fuera de la zona de cobertura de la red en general, pero dentro del rango de otros dispositivos, que pueden ser fijos o móviles. De esa manera, se pueden conectar de manera oportunista y realizar las tareas de transmisión de datos pertinentes. También son conocidas las aplicaciones de redes MANET a entornos militares [142], en donde fueron desarrolladas por primera vez estas redes, y en escenarios de recuperación frente a desastres [143]. La clave de su éxito está en que son diseñadas para un conjunto concreto de aplicaciones y que obvian los problemas de la heterogeneidad de terminales, software y usuarios, al pertenecer a un mismo proveedor. Otro campo emergente de gran éxito como especialización de redes MANET son las denominadas comunicaciones vehiculares o VANET (*Vehicular Ad-hoc NETwork*) [16]. Tanto la industria como organismos gubernamentales de distintos países apoyan la investigación de esta tecnología para todo tipo de aplicaciones: seguridad vial, gestión de tráfico, conectividad a Internet en movimiento, etc. Las redes sensoriales o redes WSN (*Wireless Sensor Networks*) son redes inalámbricas constituidas por dispositivos autónomos distribuidos espacialmente que emplean sensores para monitorizar y vigilar las condiciones físicas o ambientales del entorno, con um amplio espectro de aplicaciones. Las restricciones en cuanto a fiabilidad y temporalidad de los datos recogidos por los nodos dependen en gran medida del escenario de aplicación: militar o civil, vigilancia del entorno y del hábitat, control de incendios, salud, domótica, control de tráfico, etc.

[17] Por redes *mesh* entendemos aquellas redes cuya topología consiste en la interconexión multilateral de unos nodos con otros. Por redes multi-salto entendemos redes en las que la comunicación no se realiza de manera directa entre origen y destino de la transmisión sino que atraviesa un número variable de nodos repetidores. A veces ambos términos son usados de manera indistinta, aunque se prefiere el término multi-salto.

Más allá de sus aplicaciones, el éxito de una tecnología de redes también está determinado por la existencia de estándares ampliamente aceptados que permitan el buen funcionamiento coordinado de equipos que pueden provenir de distintos fabricantes. 802.11 [3] es el estándar del IEEE para redes inalámbricas de área local en el que se basa la popular tecnología WiFi. La familia de estándares 802.11 especifica la capa MAC y la capa física de una red WLAN. En 1997 fue adoptado el primer estándar de redes inalámbricas de área local, IEEE 802.11, con velocidades de hasta 2Mbps. El estándar inicial ha sido mejorado en distintos aspectos a través de distintos grupos de trabajo. El grupo de trabajo 802.11b produjo en 1999 un estándar WLAN de gran éxito comercial [17] con frecuencia de operación en la banda de 2.4GHz y tasas de hasta 11Mbps. Por otro lado, el grupo 802.11a publicó un estándar [18] para operar en la banda de 5GHz y con velocidades de hasta 54Mbps. Desde otra perspectiva, IEEE 802.11e-2005 o simplemente 802.11e es una enmienda que define un conjunto de mejoras en aspectos de calidad de servicio o QoS (*Quality of Service*) a través de modificaciones en la capa MAC. Estas mejoras son de importancia crítica para proporcionar aplicaciones sensibles a retardo como voz sobre IP móvil o *streaming* multimedia, es decir, para permitir cierta priorización del tráfico. Otra enmienda notable es la del grupo 802.11g, que permite trabajar en la frecuencia de 802.11b pero obtener la misma velocidad de transmisión que el estándar 802.11a mediante modificaciones en el esquema de modulación. 802.11n por su parte, mejora las tasas de transmisión introduciendo la tecnología MIMO (*Multiple Input Multiple Output*) en la capa física. 802.11i especifica mecanismos de seguridad fundamentales para proteger la comunicación y corregir la debilidad del mecanismo WEP. 802.11s [5], finalmente, es el borrador de una enmienda al estándar original para permitir a la red funcionar en modo ad-hoc en redes *mesh*. Más concretamente, extiende la capa MAC con la definición de una arquitectura que soporta tanto transmisión en modo *broadcast/multicast* como *unicast*, además de usar métricas del estado del enlace radio en topologías multi-salto. En la presente tesis se ha adoptado el estándar 802.11a, debido a que a pesar de operar en una banda de frecuencia mayor (5GHz) que 802.11b (2.4GHz), lo cual supone mayores pérdidas de propagación, esta banda está menos cargada que la de 5GHz. La Figura 3-1 muestra la arquitectura de las capas MAC y PHY en 802.11.

3.2 Capa PHY 802.11a

La capa física es el interfaz entre la capa MAC y el medio inalámbrico. Es la encargada de la transmisión y recepción de información a través de este medio, que es compartido por todos los usuarios en el caso de las redes inalámbricas. La capa física posee tres funcionalidades distintas:

- Tareas de transmisión a través del medio físico, supervisada por la subcapa PMD (*Physical Medium Dependent*).
- Intercambio de tramas con la capa MAC, lo cual se encuentra bajo el control de la subcapa física PLCP (*Physical Layer Convergence Protocol*).
- Proporcionar servicios de escucha del canal para informar a la capa MAC sobre la ocupación de éste.

A medida que las necesidades de mayores tasas de transmisión fueron aumentando, fue necesario adaptar el diseño de 802.11. En este contexto surgió 802.11a, que emplea OFDM (*Orthogonal Frequency Division Multiplexing*) como tecnología de acceso, lo cual le permite alcanzar tasas de transmisión de hasta 54 Mbps en la banda de frecuencia de 5 GHz. El uso de OFDM reduce el efecto del desvanecimiento multitrayecto[18] en recepción y aumenta la eficiencia espectral.

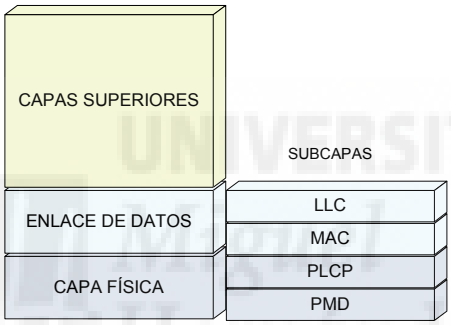


Figura 3-1. Arquitectura de capas en 802.11.

3.2.1 Subcapa PMD

La subcapa PMD es la capa más próxima al medio inalámbrico. PMD es la encargada, principalmente, de ejecutar las tareas de modulación y codificación que rige la subcapa PLCP. Entre las características distintivas de la capa física de 802.11a se encuentran el empleo de la modulación OFDM (*Orthogonal Frequency Division Multiplexing*) y la ubicación de sus canales y la potencia de transmisión permisible en cada uno de ellos.

OFDM pertenece al conjunto de modulaciones denominadas de múltiples portadoras, MCM (*Multi-Carrier Modulation*). El principio básico de funcionamiento consiste en dividir una cadena de símbolos de alta velocidad en un conjunto de cadenas paralelas de menor tasa, que son moduladas a su vez por una serie de subportadoras equiespaciadas y ortogonales, evitando de este modo la interferencia entre ellas. La ortogonalidad se

[18] El efecto del desvanecimiento multitrayecto es explicado en la sección 4.2.

consigue haciendo coincidir los máximos espectrales de cada una de las portadoras con nulos de las otras (Figura 3-2).

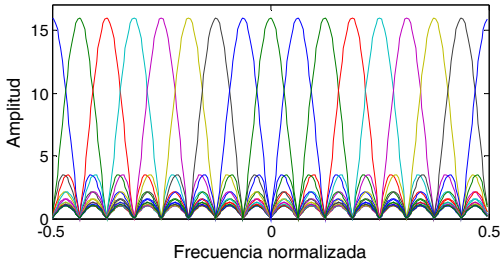


Figura 3-2. Subportadoras OFDM consecutivas.

OFDM permite el solapamiento de cada tono sin la aparición de interferencias entre ellos, lo cual mejora considerablemente la eficiencia espectral. Además, la adecuada selección del número de subportadoras y el espaciado entre ellas puede reducir de manera notable, o incluso eliminar, la interferencia entre símbolos (ISI, *Inter-Symbol Interference*) causada por la propagación multitrayecto. Esta reducción de la ISI puede conseguirse gracias a los intervalos de guarda introducidos entre símbolos OFDM. Los parámetros que caracterizan a la modulación OFDM empleada en el estándar IEEE 802.11a son (Tabla 3-1):

Parámetro	Valor
Tasa de muestreo ($1/T$) [MHz]	20
Duración del bloque OFDM (T_b) [µs]	$64*T = 3{,}2$µs
Duración del intervalo de guarda (T_g) [µs]	$16*T = 0{,}8$µs
Duración del símbolo OFDM [µs] ($T_b'' = T_g + T_b$)	$80*T = 4$
Nº de subportadoras de datos	48
Nº de subportadoras piloto	4
Espaciado entre subportadoras D_f [MHz]	$1/T_b = 0{,}3125$
Espaciado entre subportadoras exteriores [MHz]	$(N_{total} - 1)*D_f = 15{,}9375$
Tipos de modulación (velocidad de transmisión [Mbps])	BPSK (6, 9) QPSK (12, 18) 16-QAM (24, 36) 64-QAM (48, 54)

Tabla 3-1. Parámetros OFDM de IEEE 802.11a.

- Tasa de muestreo: indica el ancho de banda requerido por la modulación.
- Duración del símbolo OFDM: incluye tanto el bloque OFDM como el intervalo de guarda.

- Número de subportadoras utilizadas, distinguiendo entre las que son destinadas a datos y a señalización.
- Espaciado entre subportadoras.
- Modulaciones empleadas, que permiten alcanzar diferentes tasas de transmisión.

En cuanto a la canalización del espectro, IEEE 802.11a trabaja en la banda sin licencia de 5GHz. Esta banda es conocida como U-NII (*Unlicensed – National Information Infraestructure*). Los canales de operación y la potencia máxima a la que se debe trabajar en cada uno de ellos son determinados por las autoridades competentes (FCC, *Federal Communications Commision,* en el caso de Estados Unidos; CEPT, *European Conference of Postal and Telecommunications*, en Europa; y MIC, *Ministry of Internal Affairs and Communications*, para Japón). La siguiente tabla muestra la asignación de potencia máxima en cada una de las regiones (Tabla 3-2).

Banda [GHz]	Japón EIRP[19] [mW/MHz]	Estados Unidos [mW] [20]	Europa EIRP [mW]
4.9 – 5.091	< 10	-	-
5.15 - 5.25	< 10	40	200
5.25 - 5.35	-	200	200
5.47 – 5.725	-	-	1W
5.725 – 5.825	-	800	-

Tabla 3-2. Potencias máximas de transmisión.

3.2.2 Subcapa PLCP

Las principales tareas de la subcapa PLCP son el intercambio de tramas con la subcapa MAC, y otorgar el formato adecuado a estas tramas para que puedan ser comprensibles por la subcapa PMD. La Figura 3-3 muestra el formato en que son recibidas las tramas provenientes de la capa MAC [2]. A nivel MAC, la trama se denomina MPDU (*MAC Protocol Data Unit*) mientras que en la capa PLCP pasa a llamarse PSDU (*Physical Service Data Unit*). La trama PSDU es mapeada dentro de la trama que finalmente será enviada, denominada PPDU (*PLCP Protocol Data Unit*) en la que se incluyen las indicaciones de modulación y codificación que deben realizarse por subcapa PMD. La trama PPDU posee, principalmente, las siguientes divisiones: preámbulo, señal y datos.

[19] EIRP es la potencia radiada isotrópica equivalente, *Equivalent Isotropically Radiated Power*
[20] Máxima potencia de salida con un máximo de 6dBi de ganancia de las antenas

- Preámbulo. El preámbulo es usado como indicador de la llegada de la señal OFDM y su función es, principalmente, la de sincronizar al demodulador.
- Señal. En este campo se guarda la información que hace referencia al tamaño de la trama PSDU, bits de paridad (para corroborar la correcta recepción de la trama), y la tasa de envío de los datos. Se emplean cuatro bits (R1-R4) para codificar la tasa de envío. Las distintas posibilidades y su significado se pueden ver en la Tabla 3-3. Este campo se transmite con modulación BPSK y tasa de codificación de ½ para asegurar al máximo su correcta transmisión.
- Datos. Este campo incluye principalmente la información a transmitir, además de una serie de bits (*tail bits*) destinados a inicializar el codificador.

Tasa [Mbps]	Modulación	Tasa de Codificación [R]	R1-R4
6	BPSK	1/2	1101
9	BPSK	3/4	1111
12	QPSK	1/2	0101
18	QPSK	3/4	0111
24	16-QAM	1/2	1001
36	16-QAM	3/4	1011
48	64-QAM	2/3	0001
54	64-QAM	3/4	0011

Tabla 3-3: Tasas de transmisión posibles en IEEE 802.11a.

Como se puede observar en la Figura 3-3, a pesar de que el campo *length* de la trama PLCP posee 12 bits, y que por lo tanto permitiría hasta un total de 2^{12}-1 = 4095 bytes de datos, el tamaño viene limitado por la trama MPDU con hasta un total de 2346 bytes.

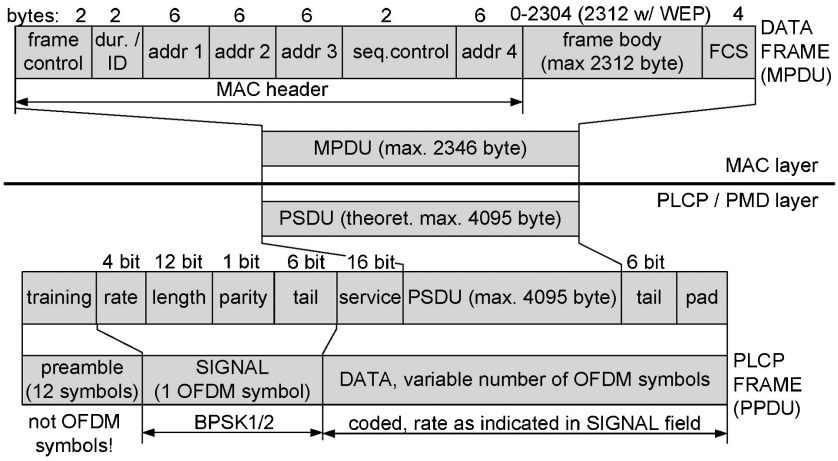


Figura 3-3. Mapeado de trama desde la capa MAC a la capa PLCP [3].

3.3 Capa MAC 802.11a

La capa MAC (Figura 3-4) proporciona servicios con control de acceso con contención y libres de contención sobre distintos tipos de capa física: infrarrojos, FHSS (*Frequency-Hopping Spread Spectrum*) y DSSS (*Direct-Sequence Spread Spectrum*). El método de acceso básico en la capa MAC de IEEE 802.11 es DCF (*Distributed Coordination Function*) que es un protocolo de acceso múltiple basado en CSMA/CA (*Carrier Sense Multiple Access with Collision Avoidance*). Además de DCF, 802.11 tiene otro método de acceso llamado PCF (*Point Coordination Function*), en el que un coordinador proporciona los derechos para la transmisión a una única estación en cada momento. Esta función no puede implementarse en una red ad-hoc, por lo que en MANET se emplea únicamente DCF.

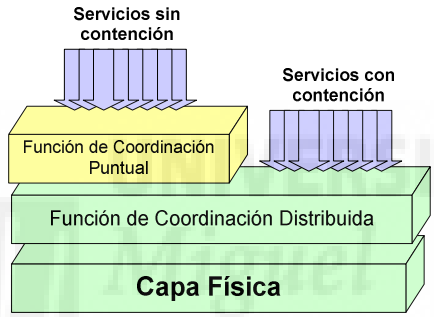
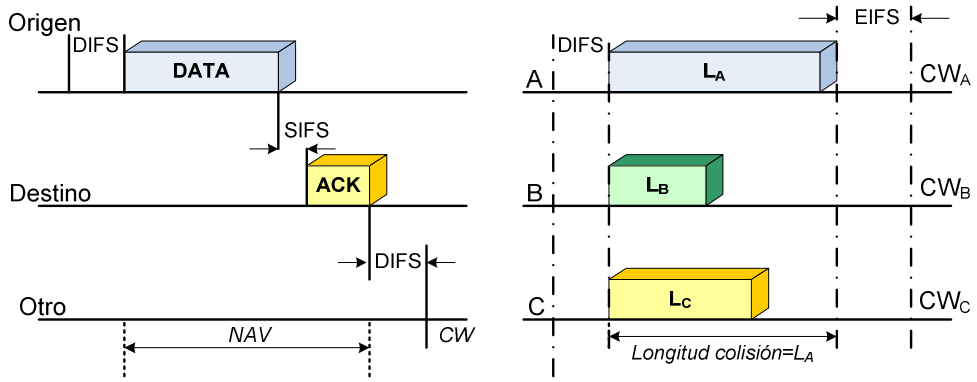


Figura 3-4. Diagrama de la arquitectura de la capa MAC 802.11.

3.3.1 Método de acceso DCF

En la Figura 3-5 se resume el funcionamiento del método de acceso al medio DCF, también llamado acceso básico. Antes de iniciar una transmisión, la estación base escucha el canal para determinar si alguna otra estación está transmitiendo. Si el medio está inactivo durante un intervalo de tiempo que excede el DIFS (*Distributed InterFrame Space*), la estación continúa con su transmisión. Las estaciones activas guardan esta información en una variable local llamada NAV (*Network Allocation Vector*), de manera que el NAV informa de cuál es el período de tiempo durante el cual el canal estará ocupado. Después de cada recepción de paquete correcta, sin errores ni colisión, el receptor espera un intervalo de tiempo SIFS (*Short InterFrame Space*), menor que el DIFS, para transmitir una trama de confirmación (ACK). Los errores son detectados mediante un algoritmo CRC (*Cyclic Redundancy Check*). Las colisiones entre transmisiones ocurren cuando dos o más estaciones comienzan a transmitir al mismo tiempo (Figura 3-5). Si no se recibe confirmación, se supone que la trama de datos se ha perdido y se procede a su retransmisión. Después de la detección de una trama errónea, el

canal debe permanecer inactivo por lo menos durante un tiempo EIFS (*Extended InterFrame Space*), antes de que las estaciones activen el algoritmo de *backoff* para reanudar sus transmisiones.



(a) Acceso básico al medio. (b) Colisión de tres paquetes.

Figura 3-5. Funcionamiento de método de acceso DCF.

Por su parte, el *backoff* es un mecanismo del estándar IEEE 802.11 para reducir la probabilidad de colisión, espaciando los comienzos de las retransmisiones para evitar las coincidencias. En concreto, se emplea una técnica de *backoff* exponencial binario ranurado. Cuando una estación *S*, con un paquete preparado para ser transmitido, observa que el canal está ocupado, retrasa la transmisión hasta el final de la misma. Cuando el canal se libera, la estación *S* inicializa un contador (llamado temporizador de *backoff*) con un valor de intervalo aleatorio, llamado intervalo de *backoff*, para programar otra vez el intento de transmisión. El temporizador decrece mientras el canal está desocupado, y se para cuando se detecta una transmisión. Se vuelve a activar cuando está otra vez desocupado durante un tiempo superior a DIFS. La transmisión de la estación empieza cuando el temporizador se agota. El tiempo que sigue a un DIFS o a un EIFS está ranurado, y las estaciones pueden comenzar a transmitir únicamente al principio de la ranura temporal correspondiente. El tiempo de *backoff* se escoge aleatoriamente en el intervalo (0, $CW - 1$), siendo CW la ventana de *backoff* o ventana de contención (*Contention Window*). En la primera transmisión, $CW = CW_{min}$, mientras que en las siguientes colisiones CW va aumentando hasta CW_{max}. Los valores de CW_{min} y de CW_{max}, dependen de la capa física específica empleada. Por ejemplo, para el sistema FHSS, CW_{min} y de CW_{max} valen 16 y 1024 respectivamente [2].

3.3.2 Sincronización

En el estándar IEEE 802.11, el conjunto de nodos conectados en modo ad-hoc entre sí, forman un conjunto IBSS (*Independent Basic Service Set*). IBSS permite que dos o más

estaciones estén conectadas entre sí sin la necesidad de un punto centralizado de control de acceso ni de ninguna infraestructura de red adicional. Para la sincronización se emplean dos funciones: (1) inicio y (2) mantenimiento de la sincronización.

- (1) Inicio de sincronización: necesaria para unirse a una IBSS ya establecida. Después del descubrimiento de una IBSS por el escaneo del medio, la estación se conecta mediante este procedimiento. Durante el escaneo el receptor se sintoniza a distintas frecuencias, buscando tramas de control que señalicen la IBSS. Sólo se inicia una nueva IBSS en caso de que no se encuentren tramas de control en el escaneo.
- (2) Mantenimiento de sincronización: para mantener la sincronización sin necesidad de una estación central se emplea un algoritmo distribuido en cada estación de la IBSS. Se basa en la transmisión de tramas de baliza con una cadencia determinada. La estación que inicia la IBSS decide el intervalo entre tramas (intervalo de *beacon*).

En cuanto al rendimiento de la capa MAC del IEEE 802.11 depende directamente de la carga de la red, es decir, del número de estaciones conectadas. Para cargas bajas, el retardo MAC es muy bajo. Sin embargo, crece considerablemente conforme la carga llega al umbral de capacidad máxima del protocolo. Esto se debe al protocolo de acceso CSMA/CA. En condiciones de carga bajas, el *overhead* es mínimo ya que el medio está casi siempre listo para transmitir. Sin embargo, para cargas elevadas, la probabilidad de colisión se incrementa y la mayoría de las transmisiones generan colisiones.

3.3.3 Protocolo RTS/CTS

En una red WLAN típica existe la posibilidad de que dos estaciones se encuentren a una distancia tal que ninguna de las dos pueda escuchar la transmisión de la otra. Se dice que están escondidas una de la otra (*hidden terminal*) [19]. El protocolo de acceso basado en la escucha de la portadora puede fallar en presencia de terminales escondidos, ya que una estación puede concluir erróneamente que el canal ha estado desocupado cuando en realidad una estación alejada puede haber estado transmitiendo, produciéndose una colisión si las dos transmiten a la vez hacia una estación intermedia (Figura 3-6).

El problema del terminal escondido puede aparecer tanto en redes *ad-hoc* como en redes con infraestructura. Sin embargo, tiene mayor gravedad en redes *ad-hoc*, puesto que tienen una escasa coordinación entre las estaciones. Para paliarlo, el mecanismo básico de acceso se amplió con el mecanismo de RTS/CTS (*Request To Send* / *Clear To Send*). En este mecanismo, después de que se gane acceso al medio y antes de que comience la transmisión de los datos, la estación transmisora envía un paquete de control corto,

llamado RTS, hacia la emisora anunciando la transmisión siguiente. El receptor debe responder con un paquete de CTS para indicar que está listo para recibir los datos. Los paquetes RTS y CTS contienen la longitud esperada de los datos. Esta información se almacena en el NAV, cuyo valor se actualiza al final del período de ocupación del canal actual. Así, todas las estaciones situadas en el rango de al menos una de las dos estaciones, sabrán que el canal estará ocupado durante el tiempo de transmisión correspondiente. Este mecanismo alivia el problema del terminal escondido y puede usarse para acaparar el canal antes de la transmisión de paquetes de larga longitud. Las únicas colisiones que se pueden producir se dan en la transmisión de los paquetes RTS y CTS, de corta longitud.

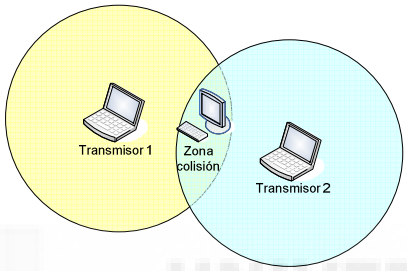


Figura 3-6. Zona de colisión por terminal escondido.

Para la correcta transmisión y recepción de un paquete no sólo hay que tener en cuenta las posibles interferencias que se produzcan, sino que hay que considerar el nivel de la señal con que se reciben el mensaje y las interferencias. En este contexto, existen tres niveles de potencia de señal en el receptor que determinan la correcta recepción de los paquetes [144]:

- Rango de transmisión (*TX_Range Transmission Range*): es el rango de valores de potencia en recepción dentro de los cuales el paquete se puede recibir y regenerar correctamente.
- Rango físico de escucha de portadora (*PCS_Range Physical Carrier Sensing Range*) es el rango dentro del cual las estaciones pueden detectar una transmisión activa.
- Rango de interferencia (*IF_Range Interference Range*) representa el rango dentro del cual la recepción de señal se ve afectada por la recepción simultánea de otra señal, de manera que la interferencia impide la correcta recepción de los paquetes.

Normalmente se cumple que: $TX\_Range \leq IF\_Range \leq PCS\_Range$

3.4 802.11s: comunicaciones *mesh* en redes multi-salto

Dentro de la familia de estándares de redes 802.11 del IEEE, el estándar 802.11s [5] está dedicado a las redes *mesh* inalámbricas. 802.11s no especifica una nueva capa física sino que se centra en la capa MAC, desarrollando funcionalidades para la gestión de redes malladas (*mesh*) tales como descubrimiento de la red *mesh*, autenticación, gestión de los enlaces *mesh*, selección de canal, seguridad, selección de camino, procedimiento de computación de la métrica del enlace, control de la congestión, *beaconing* y sincronización, etc. Por otro lado, el estándar 802.11s incluye un mecanismo de control de acceso al medio, MDA (*Mesh Deterministic Access*), y un protocolo de enrutamiento a nivel MAC híbrido, denominado HWMP (*Hybrid Wireless Mesh Protocol*) [8]. Los protocolos híbridos combinan las propiedades de protocolos de ruteo de tipo proactivo con otros de tipo reactivo. Los protocolos proactivos son aquellos en los que la ruta se establece antes de que sea inmediatamente necesaria; por lo tanto, se establecen rutas hacia todos los nodos de la red, para que en el momento que una estación necesite encaminar su información hacia cualquiera de las otras estaciones, el camino ya haya sido creado. Este tipo de protocolos es aplicable a topologías de red estáticas. Por el contrario, el tipo reactivo establece la ruta únicamente cuando la estación tiene algo que transmitir y necesita un camino para llegar a su destino. En el caso de HWMP, la combinación de estos dos tipos proporciona la flexibilidad de los protocolos reactivos y la antelación de los proactivos. La parte reactiva de HWMP se inspira en el protocolo *Ad Hoc On Demand Distance Vector* (*AODV*) [7], mientras que la parte proactiva se trata de una topología jerárquica de tipo árbol. En la presente tesis doctoral únicamente se ha hecho uso de la parte reactiva, puesto que se considera que los mecanismos de selección de ruta proactivos son más útiles en topologías básicamente estáticas, mientras que el escenario de interés de la tesis incluye movilidad de los usuarios. Por esta razón se ha implemetado el protocolo de enrutamiento DYMO [25] para la simulación de los sistemas de reputación. DYMO es una evolución del protocolo AODV, que conserva gran parte de sus beneficios y ha demostrado una mayor robustez frente a la acción de nodos egoístas en redes MANET [145]. La implementación de DYMO ha sido llevada a cabo adaptando la implementación de AODV en la extensión del Monarch Project [24] para ns-2. En esta adaptación se incluye la identidad de los nodos de la ruta en los paquetes de enrutamiento. Además, al igual que en HWMP, se permite el procesamiento de varios mensajes de enrutamiento, con el objetivo de que existan distintas alternativas entre las que seleccionar la ruta. El protocolo DYMO y la implementación realizada en esta tesis se discuten en la sección 3.5.

3.5 Protocolo DYMO

DYMO[21] [25] es un protocolo que permite realizar tareas de enrutamiento de manera dinámica, autónoma y automática entre nodos móviles que desean establecer una red MANET, tales como búsqueda de rutas a nuevos destinos, mantenimiento de rutas activas, respuesta a caídas de enlaces y cambios en la topología de la red, etc. DYMO se ha propuesto como sucesor al popular protocolo AODV, y está definido en un borrador de internet[22] de la IETF (*Internet Engineering Task Force*[23]). DYMO no añade características especiales a AODV, sino que más bien lo simplifica, manteniendo sus principios básicos de funcionamiento. Es un protocolo reactivo, lo cual quiere decir que únicamente se buscará una ruta cuando el nodo tenga algún paquete que transmitir. Como tal, se compone de dos partes: descubrimiento de rutas y mantenimiento de rutas. El proceso de descubrimiento de ruta se inicia cuando un nodo tiene algo que transmitir y no encuentra una ruta hacia el destino correspondiente en su tabla de rutas. En tal caso, difunde por la red un mensaje de búsqueda de ruta RREQ (*Route REQuest*) en modo *broadcast* (aunque el rango de difusión está limitado por un parámetro configurable incluido en el mensaje *HopLimit*). En caso de que llegue al destino, éste responde con un mensaje RREP (*Route REPly*) que se envía siguiendo el camino inverso y contiene el camino acumulado descubierto. En la tabla de rutas que cada nodo mantiene localmente, se anota información necesaria para encaminar los paquetes a través de las rutas y para su mantenimiento: dirección del nodo destino, número de secuencia para evitar lazos en las rutas, métrica de la ruta, dirección del nodo siguiente, tiempo de validez de la ruta, etc. Dentro de la parte de mantenimiento de rutas, DYMO es capaz de notificar la rotura de un enlace al conjunto de nodos afectados para que se busquen las alternativas necesarias. DYMO, al igual que AODV, utiliza un parámetro denominado número de secuencia para evaluar si la información de las rutas está actualizada y evitar lazos en las rutas. A la hora de elegir entre dos rutas distintas hacia un destino, el nodo escoge la ruta con un número de secuencia mayor (la ruta más actual). Si son iguales, y no hay riesgo de generar lazos, escoge aquella con una mejor métrica. La métrica es un parámetro que se incluye en los mensajes de búsqueda de ruta e indica el coste de enviar un mensaje al destino por esa ruta. Por defecto, se utiliza la métrica del número de saltos de la ruta, aunque pueden implementarse otras métricas. Los mensajes RERR (*Route ERRor*) notifican de la rotura de una ruta en funcionamiento. El mensaje RERR indica qué nodos destino no pueden ser alcanzados tras romperse el enlace. Los nodos precursores en las rutas caídas, que son

[21] A partir de la versión 22 del borrador de Internet de la IETF, DYMO pasa a llamarse AODVv2. En la tesis se mantiene la denominación DYMO.

[22] El borrador se encuentra actualmente en la revisión número 25 que expirará en Julio de 2013.

[23] La IETF es una organización internacional abierta de normalización, cuyo objetivo es contribuir en la ingeniería y la evolución de las tecnologías de Internet. Regula las propuestas y los estándares de Internet, conocidos como RFC.

aquellos nodos origen que utilizaban estas rutas, son notificados de la caída de las mismas para que inicien otro proceso de descubrimiento de ruta en caso necesario. Para facilitar este sistema de notificación, cada nodo puede mantener una lista de precursores, que contiene la dirección IP de los vecinos que emplean al nodo como retransmisor en sus tablas de enrutamiento. La información de la lista de precursores se recopila durante el procesado de los mensajes RREP.

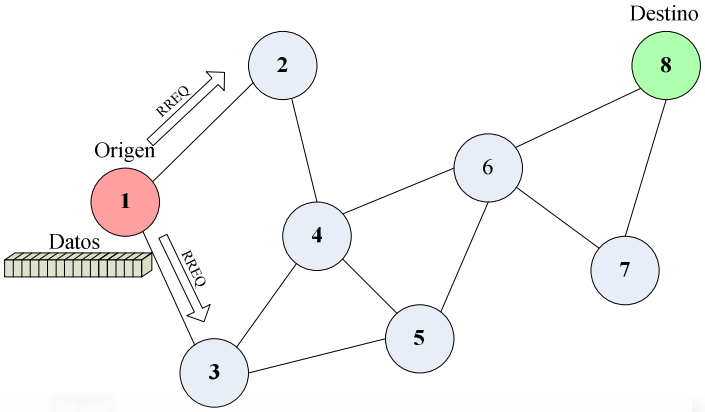


Figura 3-7. Descubrimiento de rutas, paso 1: origen comienza búsqueda de ruta.

RFC 5444 *Message Header*
AddrBlk[1,2]:= [*OrigNode*,*TargNode*]
AddrBlk.PrefixLength[*OrigNode* OR *TargNode*] (opcional)
SeqNum [*OrigNode* AND/OR *TargNode*]
Metric [*OrigNode*, *TargNode*] (opcional)
Added Node Address Block (opcional)
Added Node SeqNum
Added Node Metric[*MetricType*]

Tabla 3-4. Estructura de los mensajes de enrutamiento RREQ y RREP.

Para una mejor comprensión del funcionamiento se presenta un ejemplo concreto en el que se muestran los pasos a seguir hasta el establecimiento de una ruta mediante el protocolo DYMO. Se trata de una red multi-salto compuesta por 8 nodos o estaciones. Como se muestra en la figura (Figura 3-7), el proceso se inicia cuando una estación (*1*), el nodo *Origen*, tiene algo que transmitir. La estación consulta su tabla de ruta, por si tiene información de la ruta hasta el destino; de lo contrario, se inicia el proceso de búsqueda de ruta. Como se muestra en la Figura 3-7, el proceso se inicia, con el envío, en modo *broadcast* (o en modo *multicast*, exclusivamente a aquellas estaciones que actúen como

routers[24]), por parte del nodo *Origen* de un paquete RREQ. Este paquete contiene los campos expresados en la Tabla 3-4 (la estructura es idéntica para el mensaje de RREP):

- RFC 5444 *Message Header*: Encabezado del mensaje.
- *AddrBlk*: Este bloque contiene las direcciones IP de los nodos *Origen* y *Destino* según la Figura 3-7 (tomando el punto de vista del nodo originador del RREQ).
- *AddrBlk.PrefixLength*: Longitud del prefijo o la máscara de red.
- *SeqNum*: Contiene el número de secuencia del nodo *Origen*, el *Destino* o de los dos.
- *Metric* [*OrigNode*, *TargNode*]: Valor de la métrica de la ruta hacia los nodos *Origen* o *Destino* (dependiendo de si se trata de un mensaje RREQ o RREP).
- *Added Node Address Block*: DYMO permite incluir información de enrutamiento de otros nodos intermedios además de los nodos *Origen* y *Destino*.
- *Added Node SeqNum*: Si se incluye la información de enrutamiento de nodos adicionales, debe especificarse también el número de secuencia de dichos nodos.
- *Added Node Metric*: Valor de la métrica de la ruta hacia el nodo intermedio añadido.

En el caso de la Figura 3-7, el mensaje de RREQ originado por el nodo Origen sería el mostrado en la Tabla 3-5 (descartando los campos no relevantes para esta explicación):

AddrBlk	[*1*,*8*]
SeqNum	1
Metric	1

Tabla 3-5. Mensaje RREQ originado a partir del ejemplo en la Figura 3-7.

El mensaje originado por el nodo *Origen* alcanza los nodos *2* y *3*. Cada uno de ellos procesa el mensaje y modifica de acuerdo con la información contenida en él su propia tabla de rutas. DYMO mantiene tablas de gestión de rutas con cierta información que debe ser almacenada para cada destino conocido por el nodo. Los campos almacenados para cada entrada de ruta en la tabla son los siguientes:

- *Route.Address*: dirección del nodo destino de la ruta.
- *Route.PrefixLength*: longitud del prefijo / máscara de red.
- *Route.SeqNum*: número de secuencia de la ruta.

[24] A lo largo del trabajo, supondremos que todos los nodos en la red participan como *routers*, es decir, como potenciales retransmisores, además de poder ser origen y destino de flujos de datos.

- *Route.NextHopAddress*: dirección del siguiente nodo en la ruta.
- *Route.NextHopInterface*: tipo de interfaz del siguiente nodo.
- *Route.LastUsed*: instante en que fue utilizada por última vez.
- *Route.ExpirationTime*: instante en que caduca la ruta.
- *Route.Broken*: *flag* que se activa cuando la ruta se rompe, cuando el nodo siguiente se queda fuera del alcance o se recibe un mensaje RERR.
- *Route.MetricType*: tipo de métrica de la ruta hacia el destino.
- *Route.Metric*: valor numérico de la métrica de la ruta.

Cuando se recibe un mensaje de enrutamiento con información sobre una ruta, se comprueba si en la tabla de rutas existe alguna entrada correspondiente a esa ruta. Si no es así, se crea una entrada nueva y se extrae la información correspondiente del mensaje de enrutamiento para rellenarla. En caso de que ya exista una entrada, se realizan una serie de comprobaciones para averiguar si debe sustituirse la ruta almacenada en la tabla por la ruta correspondiente al mensaje. Se pueden dar los siguientes casos, que describen cómo es la ruta correspondiente al mensaje, respecto a la ruta almacenada en la tabla:

- No actualizada: si el número de secuencia del mensaje es menor que el número de secuencia de la ruta de la tabla, quiere decir que es más actual esta última, y por tanto no se modifica.
- Sin Garantía de Libre de Lazos: si no está asegurado que la ruta del mensaje está libre de lazos, entonces se rechaza la ruta.
- Métrica mayor: aunque los números de secuencia sean iguales y la ruta en el mensaje esté libre de lazos, si la ruta del mensaje tiene un coste mayor (cuantificado por la métrica, y que suele por defecto estar asociado al número de saltos de la ruta), entonces también se recomienda rechazar la ruta, siempre que la ruta en la tabla no esté rota. DYMO permite definir métricas alternativas a métrica por defecto.
- Alternativa mejor: si no se cumplen ninguno de los anteriores, entonces la ruta en el mensaje es mejor que la ruta en la tabla y se recomienda sustituirla.

En el ejemplo de la Figura 3-7, el mensaje de RREQ es transmitido por el nodo Origen en modo *broadcast*. Cuando los nodos *2* y *3* reciben el mensaje de RREQ, ninguno de ellos tenía información previa de una ruta hacia el nodo *1* (nodo Origen), y por tanto deben actualizar su tabla de enrutamiento (en este caso, crear una entrada nueva). La Tabla 3-8 muestra la tabla de enrutamiento del nodo *2* tras la actualización, reflejando sólo los campos relevantes para esta explicación (la tabla del nodo *3* sería similar).

Route.Address	*1*
Route.SeqNum	1
Route.NextHopAddress	*1*
Route.Metric	1

Tabla 3-6. Tabla de rutas del nodo *2* en la Figura 3-7.

Tras la actualización, los nodos *2* y *3* comprueban que ellos mismos no son el destino del mensaje RREQ, y que tampoco tienen una ruta válida hacia el mismo. Por tanto, deciden reenviar el paquete, como se muestra en la Figura 3-8. Antes de ello, deben actualizar parte de la información del paquete, tal como se muestra en la Tabla 3-7. Puede apreciarse que se ha incrementado la métrica de la ruta hacia el nodo *1* (origen del RREQ), dado que el siguiente nodo deberá dar dos saltos para llegar hasta él. También se ha incluido información de la ruta hacia el propio nodo *2*.

AddrBlk	[*1*,*8*]
SeqNum	1
Metric	2
Added Node Address Block	*2*
Added Node SeqNum	1
Added Node Metric	1

Tabla 3-7. Mensaje RREQ reenviado por el nodo *2* a partir del ejemplo en la Figura 3-8.

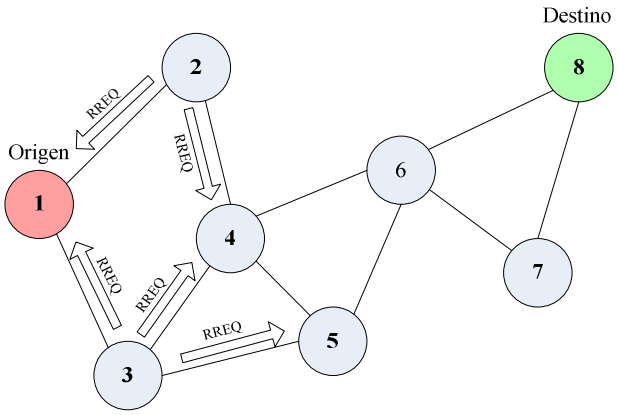


Figura 3-8. Descubrimiento de rutas, paso 2: nodos adyacentes difunden RREQ.

En la Figura 3-8 se dan tres circunstancias a tener en cuenta:

- El paquete vuelve a llegar al nodo *Origen*, donde se descarta al comprobar que este paquete había sido enviado por él mismo.

- El paquete alcanza al nodo *5*. Esta circunstancia es similar a la que se dio en el Paso 2 del modo *on-demand* en los nodos *2* y *3*.
- Y por último, la llegada del paquete al nodo *4*. Este nodo recibirá el RREQ tanto del nodo *2* como del *3*, aunque uno lo hará antes que el otro. El que llegue primero (supongamos que el *2*) provocará la creación de la entrada de la tabla de ruta y el posterior reenvío del RREQ actualizado. Cuando llegue el segundo de los paquetes, puesto que el nodo *4* ya tiene en su tabla de ruta información de cómo llegar al nodo fuente, deberá comprobar si la información recibida es mejor que la almacenada (según los pasos comentados anteriormente en esta sección). El número de secuencia será idéntico, ya que ninguno de los nodos intermedios puede aumentar el número de secuencia del mensaje. No hay riesgo de que exista un lazo en la ruta por el nodo 3, pero la métrica (el número de saltos) sería idéntica en los dos, y por tanto, el nodo *4* no enviaría un nuevo RREQ ni cambiaría la ruta hacia el nodo *1* que tiene almacenada en la tabla de rutas.

La Tabla 3.8 refleja la tabla de rutas del nodo *4* tras recibir el primer RREQ procedente del nodo *2* y con origen en el nodo *1*.

Route.Address	*1*	*2*
Route.SeqNum	1	1
Route.NextHopAddress	*2*	*2*
Route.Metric	2	1

Tabla 3-8. Tabla de rutas del nodo *4* en la Figura 3-8.

AddrBlk	[*1*,*8*]
SeqNum	1
Metric	3
Added Node Address Block	*2*
Added Node SeqNum	1
Added Node Metric	2
Added Node Address Block	*4*
Added Node SeqNum	1
Added Node Metric	1

Tabla 3-9. Mensaje RREQ reenviado por el nodo *4* a partir del ejemplo en la Figura 3-9.

En la Figura 3-9, los nodos *4* y *5* reenvían el RREQ tras haberlo actualizado, tal como refleja la Tabla 3-9, produciéndose otra vez las circunstancias anteriormente descritas en

los nodos *2*, *3*, *4*, *5* y *6*, que reciben de nuevo una copia del RREQ. Los nodos *2*, *3*, *4* y *5* lo descartarán, mientras que el nodo *6* lo reenviará a sus vecinos, de manera que alcanzará el nodo *Destino* (*8*). De no haber alcanzado el nodo *Destino*, el proceso habría seguido hasta que se alcanzara el máximo número de retransmisiones, determinado por el valor *HopLimit* incluido en el mensaje. La tabla de rutas del nodo *6* en la Figura 3-9 quedaría tal como refleja la Tabla 3-10.

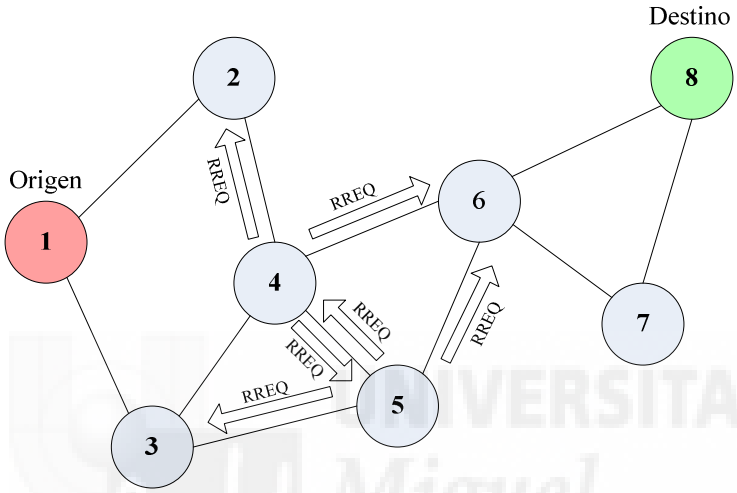


Figura 3-9. Descubrimiento de rutas, paso 3: difusión de RREQ.

Route.Address	*1*	*2*	*4*
Route.SeqNum	1	1	1
Route.NextHopAddress	*4*	*4*	*4*
Route.Metric	3	2	1

Tabla 3-10. Tabla de rutas del nodo *6* en la Figura 3-9.

Al igual que en los nodos intermedios, en el nodo destino también se puede dar la circunstancia de que lleguen más de un RREQ. En este caso, el proceso sería el mismo que el seguido por los nodos intermedios (actualización de la tabla de rutas tras el primer RREQ, tal y como refleja la Tabla 3-11 y procesamiento del resto de copias del RREQ correspondientes a rutas alternativas, si procede, con las indicaciones descritas anteriormente). La única salvedad es que el nodo destino, ante la llegada de una petición por medio del paquete RREQ, debe responder con otro paquete denominado RREP (*Route REPly*) (ver su contenido principal en Tabla 3-12). El nodo *Destino* incrementa su número de secuencia en 1 antes de trascribir dicho número de secuencia en el mensaje RREP (de ahí que *SeqNum* tenga los valores 1 y 1, que corresponden a los números de secuencia del *Origen* y del *Destino*, respectivamente). Este paquete tiene una estructura

similar al RREQ (ver Tabla 3-4). La principal salvedad es que en el caso del RREP, los nodos intermedios (*6*, *4* y *2*) ya conocen la ruta hacia el nodo *Origen*, al que va dirigido el RREP, y por tanto el mensaje se transmite en modo *unicast*. Cada uno de los nodos (*8*, 6, *4* y *2*) consulta su tabla de rutas local (ver Tablas 3-6, 3-8, 3-10 y 3-11) para saber cómo encaminar el paquete de RREP generado por el nodo *8*, tal como refleja la Figura 3-11. La Tabla 3-13 muestra la tabla de rutas[25] de cada uno de los nodos intermedios tras la actualización después de recibir el RREP procedente del nodo *Destino* (*8*). Cada uno de ellos incluye las rutas tanto hacia el nodo *Origen* como hacia el nodo *Destino*, con lo cual pueden realizar correctamente las tareas de retransmisión de los paquetes.

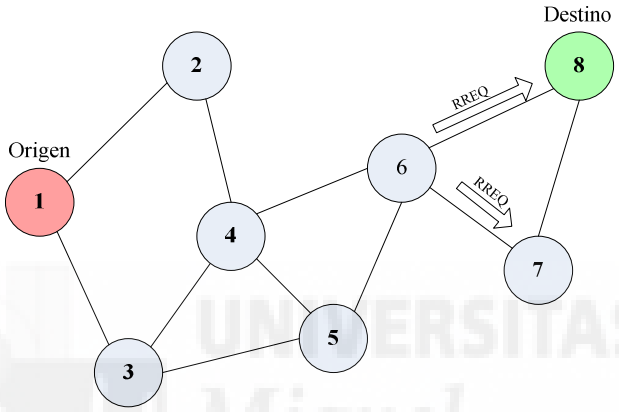


Figura 3-10. Descubrimiento de rutas, paso 4: la petición de ruta llega al destino.

Route.Address	*1*	*2*	*4*	*6*
Route.SeqNum	1	1	1	1
Route.NextHopAddress	*6*	*6*	*6*	*6*
Route.Metric	4	3	2	1

Tabla 3-11. Tabla de rutas del nodo *8* en la Figura 3-10.

AddrBlk	[*1*,*8*]
SeqNum	[1,1]
Metric	1

Tabla 3-12. Mensaje RREP generado por el nodo *8* a partir del ejemplo en la Figura 3-11.

[25] En realidad, cada nodo actualiza su tabla de rutas con cada una de las réplicas de los mensajes de enrutamiento (RREQ o RREP) que recibe, incluso aunque posteriormente descarten esas réplicas. Esto hace que las tablas de rutas reales de los nodos en el ejemplo utilizado pudieran incluir más entradas de las que aparecen en la Tabla 3-11. Sin embargo, sólo se han incluido las rutas más relevantes para el ejemplo, las que se dirigen hacia el nodo *Destino* o hacia el nodo *Origen*.

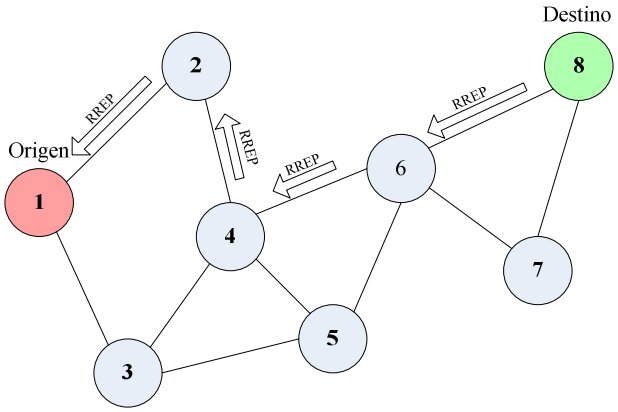


Figura 3-11. Descubrimiento de rutas, paso 5: encaminamiento del RREP en la ruta inversa.

Nodo	*6*				*4*				*2*			
Route.Address	*1*	*2*	*4*	*8*	*1*	*2*	*6*	*8*	*1*	*4*	*6*	*8*
Route.SeqNum	1	1	1	1	1	1	1	1	1	1	1	1
Route.NextHopAddress	*4*	*4*	*4*	*8*	*2*	*2*	*6*	*6*	*1*	*4*	*4*	*4*
Route.Metric	3	2	1	1	2	1	1	2	1	1	2	3

Tabla 3-13. Tabla de rutas de los nodos *6*, *4* y *2* en la Figura 3-10.

Tal y como se aprecia en la Figura 3-11, el paquete irá recorriendo los distintos nodos hasta llegar al nodo *Origen*. En este momento podemos decir que se ha completado el proceso de búsqueda de camino y que tanto el nodo *Origen* como el *Destino*, y los nodos intermedios, poseen una ruta que les conduce el uno al otro. Puede ocurrir que no fuese posible encontrar al nodo *Destino*. Si se diese esta circunstancia, el nodo *Origen* volvería, pasado cierto tiempo, a reintentar alcanzar al *Destino*, hasta un número limitado de veces (determinado por el parámetro *RREQ_RATELIMIT*). Si alcanzado dicho límite no se hubiese recibido como respuesta el RREP, la estación *Destino* pasa a tener la categoría de *Inalcanzable* y la información no podría ser enviada.

Existe además un *flag*, *DestOnly* (*Destination Only*) que puede incluirse en el paquete RREQ y varía el funcionamiento básico del protocolo DYMO. *DestOnly*=0 permite que un nodo intermedio genere la respuesta RREP anticipadamente, en vez de esperar a que el RREQ llegue al nodo *Destino* y él mismo la genere, siempre que el nodo intermedio disponga de información actualizada de cómo llegar hasta el *Destino*. Esto facilita que el nodo *Origen* sea capaz de encontrar respuesta a su petición con una menor espera, pero a su vez puede hacer que se reutilicen rutas no actualizadas. Si se selecciona *DestOnly*=1, entonces únicamente el nodo *Destino* puede generar un RREP de respuesta a los RREQ.

Además del descubrimiento de las rutas, DYMO también controla el mantenimiento de las rutas creadas y almacenadas en las tablas de los nodos. Las rutas se mantienen en

dicha tabla, mientras no ocurra algún evento por el cual deban ser eliminadas de la tabla. Si ocurre alguno de estos eventos, DYMO trata de avisar rápidamente a los nodos precursores que utilizaban esa ruta. Por nodo precusor se entiende a aquellos nodos que puedan estar utilizando como retransmisor al nodo que detecta la caída de un enlace. En la Figura 3-12, ante la caída del enlace entre los nodos *4* y *6*, el nodo *4* trata de avisar al nodo *1*. En caso de que se haya mantenido una tabla de precursores, el nodo 4 encontraría que el nodo *1* figura como precursor de la ruta caída hacia el nodo *Destino 8*. Por tanto, genera un mensaje RRER que es enviado en modo *unicast* hacia el nodo *1*. En caso de que no se dispusiera de una tabla de precursores, el mensaje de RERR se envía en modo *multicast* a todos los nodos que actúan como retransmisores.

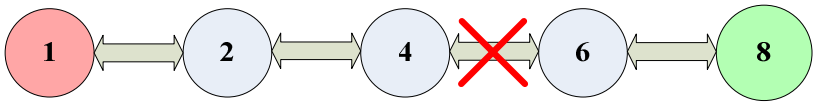


Figura 3-12. Ruptura de un enlace en la ruta.

Las causas que pueden generar la rotura de un enlace, y la generación de un mensaje de RERR son las siguientes:

- Un nodo recibe un paquete que debe retransmitir hacia un destino hacia el cual no tiene ninguna ruta en la tabla.
- Un nodo detecta la caída de un enlace en una ruta activa. Por ruta activa se entienden todas aquellas rutas que el nodo utiliza y almacena en su tabla de rutas.

Antes de utilizar una ruta de la tabla para retransmitir un paquete, los nodos realizan las siguientes comprobaciones:

- La ruta no está marcada con la etiqueta *Broken* (rota).
- La ruta no está caducada. La ruta caduca cuando se cumple que *Current_Time* > *Route.ExpirationTime*. El tiempo de expiración de la ruta (*Route.ExpirationTime*) se actualiza tras cada utilización de la misma. *Current_Time* representa el tiempo actual.
- La ruta ha permanecido inactiva durante un intervalo mayor que el permitido. DYMO define dos temporizadores referentes a los periodos de utilización de las rutas: ACTIVE_INTERVAL (pasado este intervalo sin que la ruta se haya utilizado, pasa a catalogarse como ruta inactiva) y MAX_IDLETIME (pasado el cual, una ruta inactiva pasa a expirar). Los valores de estos temporizadores se muestran en la Tabla 3-14 junto con los valores recomendados en el estándar [25] para redes pequeñas o medianas, bien conectadas y con cambios moderados de topología.

- El número de secuencia para la ruta ha caducado. El tiempo máximo de validez del número de secuencia de una ruta está determinado por el parámetro *MAX_SEQNUM_LIFETIME*.

Nombre	Valor por defecto [s]
ACTIVE_INTERVAL	5
MAX_IDLETIME	200
ROUTE_RREQ_WAIT_TIME	2
MAX_SEQNUM_LIFETIME	300

Tabla 3-14. Valores por defecto de algunos de los temporizadores usados en DYMO.

Si alguna de dichas condiciones se cumple, no se puede utilizar la ruta ni retransmitir el paquete, por lo que se generará un mensaje de RERR. En caso de que ninguna se cumpla, el paquete se retransmite y se actualiza el valor del registro de la última utilización de la ruta *Route.LastUsed*.

Cada nodo debe monitorizar la conectividad de los enlaces hacia los nodos vecinos. Para ello, puede emplear alguno/s de los siguientes métodos entre otros:

- Mecanismos de descubrimiento de vecinos [147].
- Comprobación de la caducidad de las rutas.
- Gestión de eventos de caída de enlace provenientes de una capa inferior.
- Expiración de temporizadores de TCP.

Para finalizar este apartado, a continuación se resumen las características más relevantes del protocolo DYMO para la presente tesis:

- Las rutas se establecen a petición de los nodos que necesitan transmitir datos. Estos nodos, consultan su tabla de rutas, donde registran la información necesaria sobre las rutas para retransmitir los paquetes de datos. En caso de que no encuentren la ruta que necesitan, emprenden un proceso de descubrimiento de ruta que se inicia con la propagación de mensajes de petición de ruta (RREQ). Los nodos de la red difunden el mensaje que, finalmente, puede llegar al destino. El nodo destino responde un mensaje de confirmación (RREP). Gracias a este proceso, todos los nodos intermedios que forman parte de la ruta entre los nodos extremos son capaces de aprenderla y registrarla en su tabla, y de retransmitir de un lado a otro, en modo bidireccional, los paquetes originados. Diversos mecanismos establecidos en el protocolo DYMO controlan este proceso, evitando

un aumento excesivo de la carga de señalización que supone el envío de mensajes de enrutamiento.

- En el momento de aceptar o rechazar una petición de ruta, se tienen en cuenta una serie de criterios, por orden de prioridad: en primer lugar, que esté actualizada; en segundo lugar, que no contenga lazos; y por último, se tiene en cuenta una métrica del coste de la ruta, que puede estar basada en el número de saltos, o bien en otros criterios especificados en la implementación. En las técnicas de incentivo a cooperación basadas en reputación, además de estos criterios, se tendrá también en cuenta la presencia de nodos egoístas en las rutas.
- Además del descubrimiento de las rutas, la otra función principal del protocolo de enrutamiento es el mantenimiento de las rutas en las tablas locales de los nodos. En todo momento deben vigilarse que la información de las rutas esté actualizada. Las caídas de los enlaces activos, debido a la movilidad de los nodos y a la naturaleza variable del canal radio, deben ser tratados con rapidez. Los nodos precursores que estén utilizando dichas rutas son informados mediante mensajes de RERR de que ya no están disponibles y de que deben establecerse de nuevo en caso necesario. En las técnicas de reputación, la detección de un nodo egoísta en una ruta se tratará de un modo similar a la caída de un enlace: se etiqueta la ruta como no utilizable y se avisa a los nodos precursores. Por otro lado, diversos temporizadores controlan que las rutas que no se utilizan durante un período de tiempo sean eliminadas de las tablas de rutas.

3.6 Redes celulares

Las redes de comunicaciones móviles se distinguen unas de otras por el término "generación", en inglés, *first generation*, *second generation*, etc. El nombre refleja el hecho de que existe un salto generacional considerable entre las tecnologías que las sustentan. A partir de la segunda generación, se crearon distintos organismos de estandarización cuyo objetivo es producir especificaciones para los distintos sistemas que permitan la compatibilidad entre ellos. Estos organismos son principalmente: la ITU (*International Telecommunications Union*), la ETSI (*European Telecommunication Standards Institute*), ARIB (*Alliance of Radio Industries and Business*), ANSI (*American National Standards Institute*) y 3GPP (*3rd Generation Partnership Project*).

La primera generación de sistemas móviles apareció con los sistemas analógicos o semi-analógicos de principios de los 80, denominados NMT (*Nordic Mobile Telephone*) en los países nórdicos. Por su parte, Inglaterra e Irlanda desarrollaron TACS (*Total Access Communications System*). Sus limitaciones principales eran que solamente

ofrecían servicios de voz y que eran incompatibles entre sí. La necesidad creciente de un sistema más universal dio como resultado la era de las comunicaciones móviles de segunda generación. Algunos organismos internacionales crearon un sistema con mejores servicios y con mayor transparencia y con la intención de conseguir compatibilidad global. Sin embargo, no se pudo alcanzar la implantación de un único conjunto de estándares para una red global. Los estándares en Europa diferían de los de Japón y los de América. Aún así, el sistema europeo GSM (*Global System for Mobile Communications*) ocupó un papel preponderante en un mercado que se expandió gracias a la robustez y a la relativa globalidad del sistema. GSM nació a instancias de la ETSI, el organismo creado por la Comisión Europea para crear una red global de comunicaciones móviles basada por primera vez en tecnología digital. A partir de la primera versión del estándar en 1991, GSM ha ido evolucionando adaptándose a nuevos servicios y requisitos.

UMTS es el estándar de acceso radio para las redes celulares de tercera generación. Por su parte, HSPA (*High-Speed Packet Access*) es la evolución de la tecnología de acceso radio de las redes celulares basadas en UMTS. Utiliza de forma más eficiente el espectro radioeléctrico, mejorando la velocidad y latencia en la transferencia de datos. HSPA está formado por HSDPA (*High-Speed Downlink Packet Access*) y HSUPA (*High-Speed Uplink Packet Access*), los cuales introducen mejoras para el canal descendente y ascendente respectivamente. HSPA está en continua evolución gracias al trabajo de la organización de estandarización 3GPP, que periódicamente publica las *releases*, con las especificaciones técnicas actualizadas que mejoran aspectos específicos del estándar.

3.6.1 HSDPA

HSDPA es un sistema de comunicaciones móviles de la familia de estándares HSPA que mejora algunas de las características de las redes basadas en UMTS tales como la capacidad y velocidad de transferencia de datos. Los despliegues de HSDPA actuales son capaces de alcanzar velocidades de hasta 42 Mbit/s, si bien se esperan alcanzar velocidades de hasta 337 Mbit/s con HSPA+, en la *Release 11* de los estándares del 3GPP. La Tabla 3-15 muestra una comparativa con las principales novedades introducidas en HSDPA. HSDPA introduce un nuevo canal en la capa de transporte, el HS-DSCH (*High-Speed Downlink Shared Channel*). A su vez, se introducen tres nuevos canales en la capa física: HS-SCCH (*High-Speed-Shared Control Channel*), HS-DPCCH (*High-Speed-Dedicated Physical Control Channel*) y HS-PDSCH (*High-Speed-Physical Downlink Shared Channel*). El canal HS-SCCH se emplea para informar de que está programado el envío de datos en el canal HS-DSCH. El canal ascendente HS-DPCCH transporta información de confirmación y el índice CQI (*Channel Qualitity Indicator*). Este valor numérico se envía a la estación base para indicar la calidad del enlace y cuál es

la cantidad de datos adecuada que puede mandarse en la siguiente transmisión (ver anexo A-I). El canal HS-PDSCH es el canal físico que transporta los datos de usuarios y está mapeado con el canal de transporte HS-DSCH.

Característica	UMTS Release 99	HSDPA
Canales	Nivel Transporte: DCH	Nivel Transporte: HS-DSCH
	Nivel Físico: DPDCH, DPCCH	Nivel Físico: HS-SCCH, HS-DPCCH y HS-PDSCH
Fast Power Control	Sí	No
Modulación y codificación adaptativas	No	Sí (*Link Adaptation*)
Factor de Ensanchamiento	Parámetro estático entre 4 y 512	Fijo a 16
Modulación	QPSK, DPSK, BPSK	QPSK, 16QAM, 64QAM
Scheduling	Cada TTI de 10, 20, 40 o 80ms	Cada TTI de 2ms a nivel de BTS
Retransmisiones	Retransmisiones a nivel de RLC	HARQ – Retransmisiones a nivel físico
Soft handover	Sí	No. Transmisión desde una única celda servidora

Tabla 3-15. Comparativa de características de UMTS y HSDPA.

El mecanismo de *Link Adaptation* es muy dinámico, ya que opera cada 2ms. El canal HS-DSCH descendente se comparte entre los usuarios para hacer un uso más eficiente de los recursos radio, teniendo en cuenta las condiciones del canal para cada uno. Cada terminal de usuario transmite continuamente con cada TTI de 2ms una indicación (CQI) de la calidad de la señal del canal descendente. Teniendo en cuenta este valor, la carga y la capacidad de la celda, y el tipo de terminal de usuario, la estación base programa qué usuarios utilizarán el canal en la siguiente ranura de 2ms, y cuántos datos mandarán cada uno, adaptando la codificación, la modulación y el número de códigos. El esquema de modulación más robusto utilizado es QPSK (*Quadrature Phase-Shift Keying*), aunque con unas buenas condiciones del canal es posible utilizar la modulación 16QAM (*Quadrature Amplitud Modulation*) y 64QAM, con lo que la velocidad de transmisión de datos se incrementa considerablemente (ver anexo A-I). La asignación de códigos la determina la estación base. Con un factor de ensanchamiento en HSDPA fijo a 16, se obtienen un total de 16 códigos de canalización, de los cuales 15 pueden ser asignados al canal HS-DSCH.

HSDPA incorpora el mecanismo de retransmisión híbrido HARQ (*Hybrid Automatic Repeat-reQuest*). Si se requiere la retransmisión de un paquete, el terminal guarda el paquete original y lo combina con el paquete retransmitido. Dos paquetes recibidos con error pueden combinarse y dar lugar a un paquete sin error, aumentando la eficiencia del proceso. Se especifican dos modalidades: *chase combining* (ambos paquetes son idénticos), e *incremental redundancy* (paquetes diferentes). Las retransmisiones HARQ se procesan en el nivel físico en la estación base, reduciendo así su tiempo RTT (*Round-Trip Time*).

4

Entorno de evaluación

El funcionamiento de las técnicas propuestas en esta tesis ha sido evaluado a través de simulaciones. En este capítulo se abordan aspectos relacionados con el modelado y la simulación de una red de comunicaciones inalámbricas, como herramienta para la comprobación del funcionamiento y del rendimiento de las técnicas estudiadas en el presente trabajo. La creciente disponibilidad de computadores y potentes estaciones de cálculo hacen de las técnicas de modelado y simulación una atractiva alternativa para la validación experimental de resultados teóricos en distintas áreas de investigación. Por ello, en el área de las redes de comunicaciones, resulta usual recurrir a este tipo de técnicas, dada la inviabilidad económica de la implementación real de grandes redes destinadas únicamente a fines de investigación. También resulta muy comprometida la implementación en redes comerciales de protocolos y técnicas en fase experimental. Mediante la simulación, es posible hacer pruebas a gran escala y lo suficientemente exactas en sus resultados para validar o desechar algunas opciones de diseño de protocolos. Todo ello hace aconsejable la utilización de la simulación como herramienta de validación de las propuestas de investigación. Por tanto, los experimentos del presente trabajo se han llevado a cabo mediante simulación.

Un aspecto fundamental en los estudios basados en simulación es escoger y utilizar los modelos adecuados para emular el funcionamiento de los parámetros clave reales, con el

fin de obtener resultados y conclusiones válidas y precisas. Por esta razón, en esta tesis se ha empleado una plataforma de simulación de sistemas de comunicaciones que es ampliamente utilizada en la comunidad científica, y se han empleado modelos detallados de intereferencia y de propagación en el canal radio, los cuales también han sido validados en otros estudios. Este capítulo presenta la plataforma de comunicaciones empleada en esta tesis, detallando su estructura y las modificaciones realizadas para simular el funcionamiento de redes MANET en presencia de nodos egoístas y técnicas de incentivo a cooperación. Además, se presentan los principales escenarios considerados en la tesis.

4.1 Simulador de comunicaciones ns-2

Para la investigación en redes MANET se necesitan simuladores de comunicación que modelen adecuadamente el funcionamiento de los protocolos de comunicaciones y las tecnologías de red, el movimiento de los nodos, los protocolos de comunicación y la propagación por radio. Si bien existen distintas alternativas en la comunidad científica, en esta tesis se ha escogido la plataforma ns-2 [20]. ns-2 ha sido ampliamente validada en multitud de estudios científicos, y recibe gran atención por parte de la comunidad científica, que mantiene distintos sitios webs en donde se contribuye, actualiza y amplía el código fuente. Su amplia aceptación, flexibilidad y la posibilidad de modificar el código para implementar nuevos protocolos y mejorar los existentes han sido factores determinantes a la hora de escoger esta plataforma.

4.1.1 Descripción y funcionalidades

La plataforma de simulación empleada en esta tesis está basada en ns-2 versión 2.29 (ns-2.29, 22 de Octubre de 2005)[26] con algunas mejoras adicionales, y actualizaciones proporcionadas por otros autores. El *Network Simulator 2* (ns-2) fue desarrollado por el *Information Sciences Institute* de la *University of Southern California*. Es una herramienta versátil para la investigación en redes de comunicaciones que puede ser configurada para simular un amplio rango de tecnologías de redes y distintos protocolos de comunicación:

- Tecnologías de red tanto cableadas como inalámbricas (locales y por satélite, exceptuando las comunicaciones móviles celulares).

[26] Se ha utilizado esta versión de ns-2 porque además de incluir los protocolos y los módulos necesarios para llevar a cabo las simulaciones en redes MANET correspondientes a la parte experimental de esta tesis, también se disponía, para esta versión, de código contribuido por otros investigadores que mejoraba los modelos de propagación radio de ns-2 disponibles en la distribución oficial. Estos modelos eran imprescindibles para lograr los objetivos de esta tesis.

- Protocolos de transporte tales como TCP y UDP.
- Generación de comportamientos de tráfico FTP, Telnet, Web, CBR y VBR.
- Simulación de mecanismos de gestión de colas en routers tipo Drop Tail, RED y CBQ.
- Soporte para diversos tipos algoritmos de enrutamiento
- Modelos de movilidad para simulación de redes inalámbricas

En la Tabla 4-1 se muestran algunos de los protocolos de comunicación y los modelos de tecnologías de comunicación incluidos en la versión de ns-2 utilizada en esta tesis. Además de los módulos ya incluídos en la distribución oficial, están disponibles otros adicionales como código contribuido [21], cuyo contenido es mantenido por usuarios y puede ser utilizado junto con la distribución de oficial.

Nivel	Protocolos y módulos
Aplicación	Ping, telnet, FTP, multicast FTP, HTTP, webcache
Transporte	TCP (distintas variaciones), UDP, SCTP, XCP, TFRC, RAP, RTP Multicast: PGM, SRM, RLM, PLM
Red	*Unicast*: IP, MobileIP, vector de distancia y estado de enlace, IPinIP, enrutamiento en origen, Nixvector. *Multicast*: SRM, centralizado MANET: AODV, AOMDV, DSR, OLSR, DSDV, TORA, IMEP
Enlace	ARP, HDLC, GAF MPLS, LDP, Diffserv Gestión colas: DropTail, RED, RIO, WFQ, SRR, *Semantic Packet Queue*, REM, *Priority*, VQ MAC: CSMA, 802.11, 802.11.1 (WPAN), *satellite Aloha*
Físico	Modelos propagación radio: *TwoRay*, *Shadowing*, *Nakagami*, *OmniAntennas*, *EnergyModel*, *Satellite Repeater*

Tabla 4-1 Protocolos y modelos de tecnologías de comunicación en ns-2.

4.1.2 Arquitectura básica

ns-2 es un simulador de eventos discreto que opera a nivel de paquete, desde el nivel de enlace hacia capas superiores y permite simular redes cableadas e inalámbricas. Está disponible para casi todas las plataformas basadas en UNIX (FreeBSD, Linux, Sun Solaris) y también puede ejecutarse en Windows (con el emulador cygwin). ns-2 también es un simulador orientado a objetos, escrito a la vez en C++ y en lenguaje OTcl. OTcl es una evolución de tcl con extensiones de lenguaje orientado a objetos, que permite definir

clases y crear objetos de esas clases. La parte de OTcl se emplea como interfaz hacia el usuario. Su estructura se basa en una jerarquía de clases en C++ (llamada también jerarquía compilada) y una jerarquía similar de clases dentro del intérprete OTcl (llamada también jerarquía interpretada). Ambas están estrechamente relacionadas. Desde el punto de vista del usuario, existe una correspondencia exacta uno a uno entre una clase en la jerarquía interpretada y en la jerarquía compilada. El fundamento de esta jerarquía es la clase *TclObject*. Los usuarios crean nuevos objetos a través del intérprete; dichos objetos son instanciados dentro del intérprete y se reflejan en la creación de un objeto equivalente en la jerarquía compilada. Además, existen algunas jerarquías dentro del código C++ y de los scripts de OTcl que no están enlazadas, es decir, no tienen su correspondencia en el otro lenguaje. Grosso modo, OTcl hace de interfaz hacia el usuario para tareas de configuración, con soporte de objetos, mientras que tclcl hace de enlace entre C++ y OTcl. La razón de esta implementación basada en diversos lenguajes se debe a la doble orientación de la herramienta [22]. Por un lado, está orientado a la simulación detallada de protocolos, lo cual requiere un lenguaje de programación de sistemas que maneje eficientemente grandes conjuntos de datos, bytes, encabezados, etc. Para estas tareas, el tiempo de ejecución es más importante que el tiempo de preparación. Por otro lado, en muchos casos la investigación de sistemas y redes de comunicación consiste en la simulación de escenarios en los que varían ligeramente la configuración o los valores de ciertos parámetros. En estos casos, es más importante el tiempo de iteración, es decir, el que se emplea en cambiar el modelo y volver a lanzar las simulaciones. Lo ideal en este caso es poder lanzar simulaciones desde un script en el que automáticamente se cambian los parámetros de los escenarios de acuerdo a los aspectos que se quieren evaluar. Con los dos lenguajes de ns-2 se llega a un compromiso entre ambos aspectos: C++ es más rápido en ejecución pero de modificación más lenta, mientras que OTcl puede ser modificado interactivamente y controlado a través de scripts, aunque su ejecución sea comparativamente lenta. La unión entre ambos se realiza a través de tclcl [23].

Los elementos que forman el simulador ns-2 pueden dividirse en tres categorías:

- La librería de componentes de red (*Network Component*).
- La librería de interconexión de objetos (tcl / otcl / tclcl).
- El programador de eventos (*scheduler*).

Los componentes de red constituyen los elementos que forman la red, tal como nodos, enlaces o colas. Su interconexión, definida en las librerías de interconexión, define el camino que seguirá un paquete en la simulación. Estos componentes de red pueden ser simples, creados directamente a partir de su clase de C++, o compuestos, formados por la interconexión de múltiples componentes simples. En general, todos los componentes de red en ns-2 se crean, se conectan y se configuran desde el código OTcl. El programador

de eventos se encarga de gestionar el orden en el que se ejecutan los eventos de la simulación. Un evento en ns-2 viene definido por un instante de tiempo, un identificador único, un puntero al siguiente evento que debe ejecutarse, y un *handler* o manipulador, que apunta al objeto que deberá emprender el evento en el instante de tiempo indicado. Los eventos se colocan en una cola ordenada por tiempo y se ejecutan uno a uno bajo la gestión del programador de eventos. Todos los componentes de red son una sub-clase de la clase *Handler* (programador de eventos), puesto que requieren ejecutar eventos como la entrega o recepción de paquetes, etc.

4.1.3 Proceso de simulación en ns-2

Para evaluar los protocolos de incentivo a cooperación en redes inalámbricas en esta tesis se ha seguido el proceso siguiente: en primer lugar, se debe construir el escenario en donde está desplegada la red, formada por usuarios peatones. Se debe determinar la disposición de edificios en el escenario que determinarán las condiciones de visibilidad, así como el recorrido realizado por los peatones, también condicionado por la disposición de los edificios. En segundo lugar, se ejecuta ns-2 con un script OTcl de configuración y con el recorrido de los peatones y la topología del escenario como entradas. En el *script* deben incluirse las instrucciones necesarias para iniciar el programador de eventos, crear la topología de red, empleando los componentes de red y los mecanismos de interconexión necesarios, y crear los elementos generadores de tráfico. En el script se especifican los diferentes valores que deberán tomar los parámetros de entrada que quieran estudiarse. Los resultados de la simulación generada con ns-2 deben ser analizados con una herramienta externa e interpretados para evaluar el rendimiento la técnica en estudio. Finalmente, de los resultados se extraerán las conclusiones más relevantes en función de las técnicas empleadas y de la configuración de los parámetros de entrada, y serán reflejados en gráficas y tablas. Este será el procedimiento general; los detalles específicos de configuración se proporcionarán en cada uno de los capítulos experimentales.

La estructura fundamental de un archivo *script* de simulación en OTcl para ns-2 deberá contener los siguientes puntos:

- Definición de variables de configuración del escenario.
- Configuración de los parámetros de los objetos de C++.
- Creación del objeto de simulación.
- Creación y configuración de la topología de red.
- Creación y configuración de los agentes de ruteo y aplicación.
- Inicialización y fin de la simulación.

4.2 Implementación de sistemas de comunicaciones inalámbricos en ns-2

La simulación de redes inalámbricas de nodos móviles se lleva a cabo gracias al modelo inalámbrico de ns-2, originalmente importado como una extensión de movilidad desarrollada por *CMU's Monarch Group* [24]. El modelo CMU original permitía simulaciones de redes WLAN así como redes *ad hoc* multi-salto. Posteriormente, fueron introducidas extensiones para poder simular redes cableadas e inalámbricas combinadas. Además, fue incorporada una extensión para *MobileIP*.

La implementación de la parte inalámbrica de la red en ns-2 se compone principalmente de los tres bloques que se muestran en la Figura 4-1: nodo móvil, canal inalámbrico, antenas y propagación. Esta implementación sigue un enfoque por capas en la que los módulos están interconectados para el intercambio de paquetes.

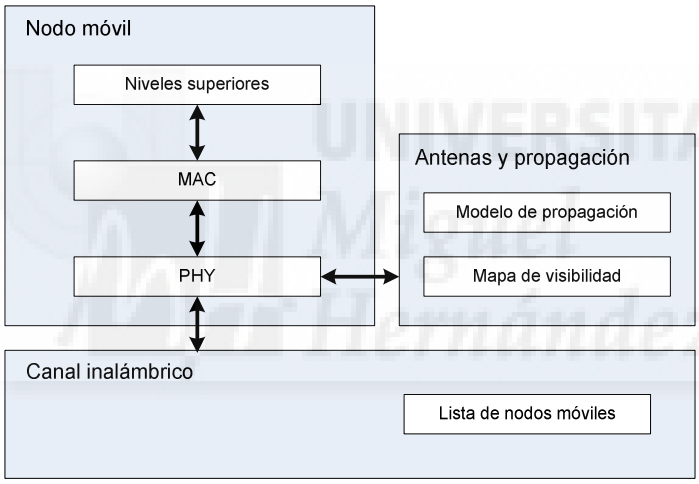


Figura 4-1. Módulos de Nodo móvil, Canal inalámbrico y Antenas y propagación en ns-2.

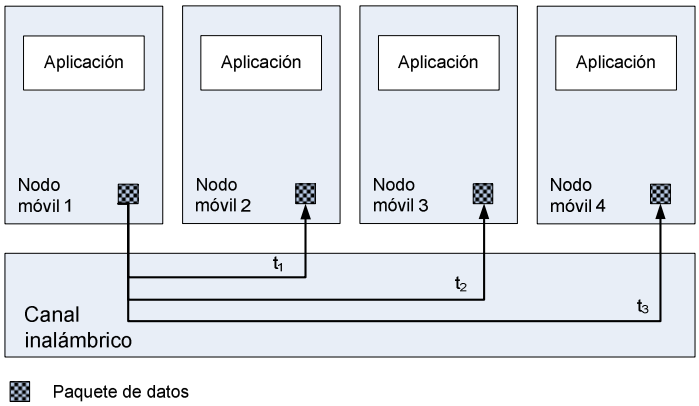


Figura 4-2. Funcionamiento del canal radio en ns-2.

Canal inalámbrico: este bloque interconecta todos los nodos móviles que operan en el mismo canal, como se ilustra en la Figura 4-2. Cuando un nodo móvil transmite un paquete a través del canal inalámbrico, este bloque crea una copia del paquete en la interfaz PHY de cada nodo móvil, con un retardo de propagación proporcional a su distancia al transmisor. Cada nodo a continuación, es programado para comenzar a recibir la copia del paquete en un instante diferente, teniendo en cuenta los retrasos experimentados por los diferentes nodos a diferentes distancias desde el transmisor. En recepción, cada nodo será el responsable de determinar si recibe correctamente el paquete o no. La decisión de la correcta recepción viene marcada por la relación señal a ruido e interferencia (SINR *Signal to Interference and Noise Ratio*) con la que es recibido el paquete, tal y como se explicará en el apartado 4.3 (Interfaz física) de este capítulo. A la hora de entregar los paquetes, se ordenan en función de la distancia al nodo transmisor. Así, el nodo más cercano será el primero en recibir el paquete a través de su interfaz física, simulando, de este modo, el retardo producido por la propagación real del paquete.

Nodo móvil: este bloque implementa las diferentes capas de comunicación disponibles en un nodo inalámbrico, junto con funciones de movilidad para actualizar la posición de los nodos cada vez que se recibe un nuevo paquete. Los módulos más importantes del nodo móvil en esta tesis son PHY y MAC, que son tratados en apartados posteriores. La Figura 4-3 muestra el diagrama de bloques de un nodo móvil asociado a un canal radio. El objeto que implementa el nodo móvil se deriva del objeto nodo genérico, añadiendo principalmente la funcionalidad de movilidad y permitiendo su asociación al canal radio. Los distintos componentes de red que implementa la clase nodo móvil (*class mobilenode*) son:

- PHY (interfaz física): encargada de recibir los paquetes procedentes del canal y pasárselos a la capa MAC en caso de recibirlos correctamente. Se describe más adelante en el apartado 4.3. En el presente trabajo se ha empleado la interfaz física del estándar 802.11a.
- MAC (control de acceso al medio): implementa el protocolo MAC de IEEE 802.11a para el caso de la función de coordinación distribuida (DCF).
- IFQ: cola de salida de los mensajes.
- LL: capa de enlace asociada al bloque ARP (*Address Resolution Protocol*). Se encarga de la búsqueda de la dirección MAC del nodo destino a partir de su dirección IP. Esta capa es la encargada de pasar en sentido descendente los paquetes a la cola IFQ y, en sentido ascendente, los pasa directamente a la capa de ruteo.
- Agente de ruteo: encargado de dar soporte al sistema para que puedan establecerse comunicaciones multi-salto entre distintos nodos. El agente de

ruteo proporciona las funcionalidades necesarias para llevar a cabo el enrutamiento de paquetes de datos a cualquier nodo de la red. Actualmente, la versión de ns-2 implementa los protocolos DSDV, DSR, TORA y AODV, protocolos generalmente utilizados en redes MANET.

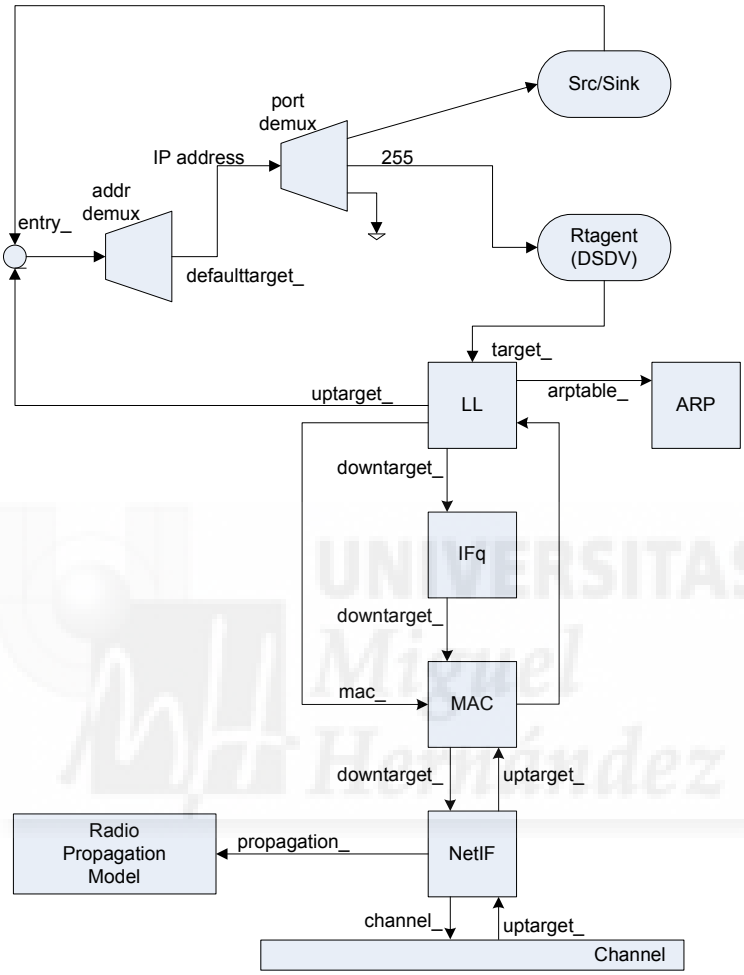


Figura 4-3. Diagrama de bloques de un nodo móvil asociado a un canal radio.

En la Figura 4-3 también pueden observarse los componentes que la clase nodo móvil hereda de la clase nodo genérico. Estos componentes consisten en un objeto de entrada, un clasificador de direcciones, y un clasificador de puertos a los que se asocian agentes y aplicaciones. Los objetos Agente y Aplicación han de conectarse a los nodos para la generación, procesado y recepción del tráfico de datos. Mientras que los agentes representan puntos terminales en la red, las aplicaciones son objetos que generan la información y se encuentran por encima de los agentes en la pila de protocolos de comunicación.

Antenas y propagación: La capa PHY hace uso del módulo de antenas y propagación para determinar el nivel de potencia recibida de cada paquete, que calcula en función del

modelo de propagación considerado. El nivel de detalle del modelo de propagación radio es un aspecto importante debido a que puede afectar considerablemente a los resultados y conclusiones del estudio. En general, los modelos de propagación de radio para investigaciones a nivel de sistema deben reflejar adecuadamente los efectos de la pérdida básica de propagación (*PL Path Loss*), desvanecimiento lento o *shadowing* (*SH SHadowing*) y desvanecimiento por multitrayecto o *multipath fading* (*MP Multi Path fading*) [148]. La pérdida básica de propagación representa la media local de la potencia de la señal recibida con respecto a la potencia de transmisión como una función de la distancia entre el emisor y el receptor. El desvanecimiento lento modela el efecto de los obstáculos próximos al receptor en la potencia media de la señal, a una determinada distancia. El desvanecimiento multitrayecto es consecuencia de la recepción de varias réplicas de la señal transmitida en el receptor. Teniendo en cuenta la potencia de transmisión (*Pt*), y los efectos de propagación, la potencia de señal recibida (*Pr*), puede calcularse en dB, usando la siguiente ecuación, que considera ganancias unitarias de antena y con pérdidas despreciables de circuito:

$$Pr = Pt - PL - SH - MP \tag{4-1}$$

Los distintos modelos de propagación radio proporcionan expresiones para calcular valores de *PL*, *SH* y *MP* en función de distintos parámetros. Debido a la relevancia de los modelos de propagación radio para los propósitos de esta tesis, la presentación detallada de los distintos modelos de propagación disponibles en ns-2 se realiza a continuación en la sección 4.2.1

4.2.1 Modelos de propagación

El simulador ns-2 incluye tres modelos de propagación diferentes: propagación en espacio libre (*FreeSpace*), propagación de dos rayos (*TwoRayGround*), y un modelo de propagación denominado *Shadowing*. Todos ellos modelan el efecto de las pérdidas básicas de propagación o *pathloss* mediante una función logarítmica dependiente de la distancia (*log-distance pathloss*). Por su parte, la característica distintiva del modelo *Shadowing* es que modela el efecto del desvanecimiento lento. Las ecuaciones de *pathloss* para cada uno de estos tres modelos vienen representadas en la Tabla 4-2. En las expresiones, h_T y h_R representan las alturas de las estaciones transmisora y receptora, mientras que λ es la longitud de onda de la señal portadora (en metros). El modelo de propagación *FreeSpace* es totalmente determinista y produce unas pérdidas en la señal proporcionales al cuadrado de la distancia entre transmisor y receptor (d^2). El modelo *TwoRayGround*, también determinista, reproduce las mismas pérdidas que el modelo *FreeSpace* hasta cierta distancia crítica d_c, a partir de la cual, las pérdidas tienen una

dependencia de orden cuatro con la distancia (d^4). En cuanto al modelo de propagación *Shadowing*, como puede observarse en la expresión, las pérdidas básicas de propagación son configurables a partir del parámetro *n* (exponente de *pathloss*). Además, este modelo permite ajustar el impacto que producen los obstáculos en la señal mediante la modificación de la desviación típica (σ) del desvanecimiento lento. Los valores típicos de *n* y σ para el modelo *Shadowing* se muestran en las Tablas 4.3 y 4.4.

Modelo ns-2	*PL* [dB]	*SH* [dB]
FreeSpace	$PL(d[m]) = 10\log_{10}\left(\frac{d^2(4\pi)^2}{\lambda^2}\right)$	-
TwoRayGround	$PL((d[m]) = \begin{cases} 10\log_{10}\left(\frac{d^2(4\pi)^2}{\lambda^2}\right) & si \quad d < d_c \\ 10\log_{10}\left(\frac{d^4}{h_T^2 h_R^2}\right) & si \quad d \geq d_c \end{cases}$ donde $d_c = \frac{4\pi h_T h_R}{\lambda}$	-
Shadowing	$PL(d[m]) = 10\log_{10}\left(\frac{d}{d_0}\right)^n$	$N(0, \sigma^2)$

Tabla 4-2. Modelos de pérdidas básicas de propagación incluidos en ns-2.

Entorno de propagación		*n*
Exterior	Espacio libre	2
	Entorno urbano	2.7 a 5
Interior	Visión directa	1.6 a 1.8
	Sin visión directa	4 a 6

Tabla 4-3. Valores típicos del exponente de *pathloss* del modelo de propagación *Shadowing.*

Entorno de propagación	σ
Exterior	4 a 12
Interior (oficinas)	7 a 9.6
Interior (fábricas)	3 a 6.8

Tabla 4-4. Valores típicos de la desviación típica del desvanecimiento del modelo de propagación *Shadowing.*

La mayoría de los trabajos consultados emplean un modelado del canal radio relativamente sencillo, que considera únicamente el efecto *pathloss* (ver Tabla 2-6). En este proyecto, con el objetivo de cuantificar la influencia de un modelo de propagación realista, ha sido incluido el modelo de propagación micro-celular de entorno urbano

publicado en [26], que no sólo considera pérdidas por *pathloss* y *shadowing*, sino también desvanecimiento rápido por propagación multitrayecto (*multipath fading).* El modelo micro-celular es el modelo de propagación que más se aproxima al modelo idóneo para el presente trabajo, puesto que considera las alturas de las antenas relativamente reducidas, situadas a 5 metros de altura (en este trabajo se supone que las antenas están ubicadas en cada terminal móvil, por lo tanto se acepta una altura media de 1,5m.), las velocidades de desplazamiento de los peatones y un entorno de propagación urbano. La implementación de dicho modelo, obtenido de [26], está basado en la clase *ShadowingVis* de ns-2, que diferencia las condiciones de propagación LOS (*Line Of Sight* o visión directa) y NLOS (*Non Line Of Sight* o no visión directa) entre transmisor y receptor, tal y como presenta la Figura 4-4.

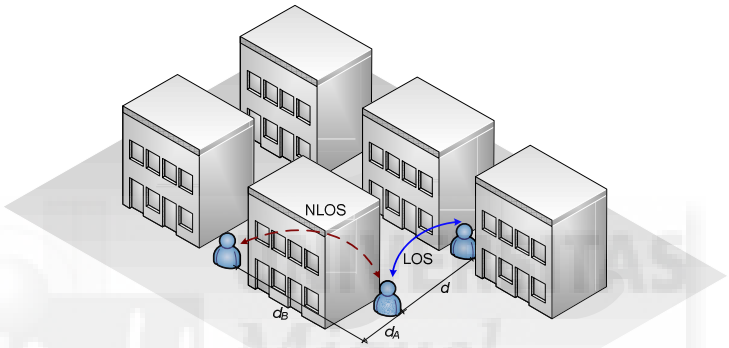


Figura 4-4. Condiciones LOS y NLOS en entorno urbano.

Según este modelo, las pérdidas básicas de propagación en condiciones LOS dependen de la distancia entre transmisor y receptor d, de la altura de sus respectivas antenas (h_A y h_B), y la longitud de onda λ, todas ellas en metros, y de la frecuencia de transmisión (f en GHz):

$$PL_{LOS}(d) = \begin{cases} 22.7\log_{10}(d) + 41 + 20\log_{10}(f/5) & si \quad d < R_{bp} \\ 40\log_{10}(d) + 41 - 17.3\log_{10}(R_{bp}) + 20\log_{10}(f/5) & si \quad d \geq R_{bp} \end{cases} \tag{4-2}$$

donde

$$R_{bp} = 4\frac{(h_A - 1)(h_B - 1)}{\lambda} \tag{4-3}$$

Sin embargo, para condiciones NLOS, la estimación de las pérdidas básicas de propagación no viene determinada por la distancia euclídea entre transmisor y receptor, sino por la distancia real que recorrería la señal, teniendo en cuenta el entorno en el que

se encuentra. Como puede observarse en la Figura 4-4, en condiciones NLOS la estimación de las pérdidas básicas de propagación dependen de las distancias d_A y d_B (distancias en metros desde los nodos móviles hasta la intersección). De esta manera, las pérdidas básicas de propagación en transmisiones sin visión directa vienen definidas por la ecuación 4.4.

$$PL_{NLOS}(d_A, d_B) = PL_{LOS}(d_A) + 20 - 12.5n_j + 10n_j \log_{10}(d_B) \tag{4-4}$$

donde

$$n_j = \max(2.8 - 0.0024d_A, 1.84) \tag{4-5}$$

Este modelo sigue utilizando una distribución aleatoria *log-normal* de media nula y desviación típica σ para modelar el desvanecimiento lento producido por la presencia de obstáculos entre transmisor y receptor. En particular, en [26] son propuestos los valores σ=*3dB* y σ=*4dB* para condiciones de propagación LOS y NLOS, respectivamente. El efecto de la propagación multitrayecto es modelado para condiciones LOS mediante una distribución aleatoria Ricean, mientras que para condiciones NLOS se considera una distribución Rayleigh.

En un entorno de propagación realista el desvanecimiento lento que sufre una señal no varía de forma rápida, ya que los obstáculos entre transmisor y receptor no varían su posición de forma inmediata. En otras palabras, existe un nivel de correlación no nulo en el desvanecimiento de las señales transmitidas. A modo de ejemplo, puede observarse en la Figura 4-5 el efecto combinado de las pérdidas básicas de propagación, el desvanecimiento lento correlado, y el efecto del multitrayecto sobre el nivel de potencia recibida por un nodo móvil bajo condiciones NLOS.

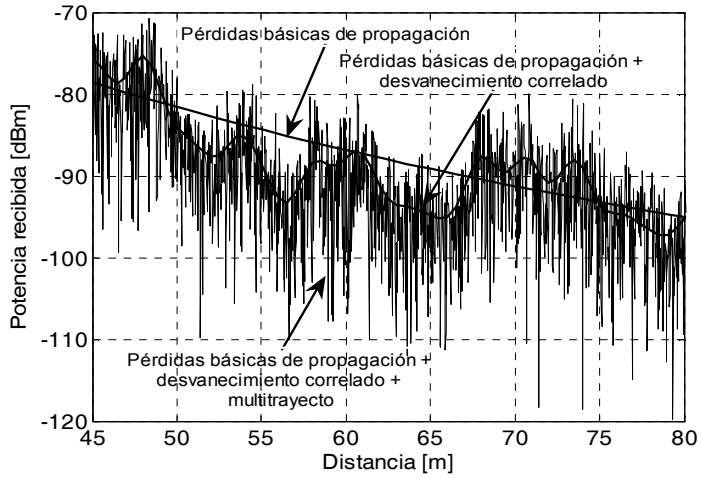


Figura 4-5. Efectos de la propagación radio en condiciones NLOS.

Para el cálculo de la potencia con la que se reciben los paquetes de datos es necesaria también la configuración de la antena, que será empleada en la transmisión y recepción de los paquetes. ns-2 únicamente permite el empleo de antenas omnidireccionales, posibilitando la configuración tanto de la posición relativa de la antena respecto al nodo como de su ganancia.

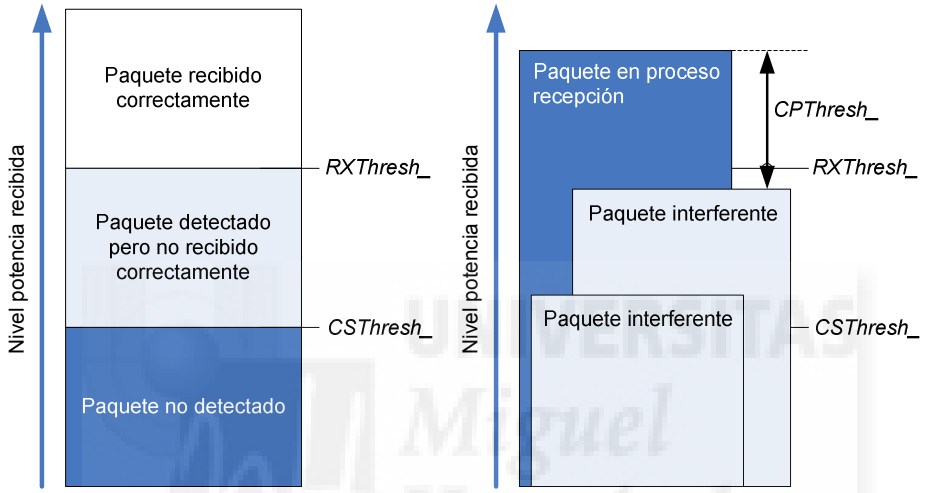
4.2.2 Capa PHY 802.11 en ns-2

El módulo PHY es responsable del manejo de los paquetes recibidos desde el canal inalámbrico. La interfaz de los nodos con el canal radio viene implementada en la clase *Phy/WirelessPhy*. La actual implementación de ns-2 permite definir de forma general, para todos los nodos, la tasa de transmisión de datos, la frecuencia portadora de la señal, la potencia de transmisión, y una constante de pérdidas de la propia interfaz (debidas a conexiones, cables, etc.). Todos estos parámetros son configurados en código OTcl en el script de la simulación y presentan la estructura mostrada en la Figura 4-6. Como puede observarse en la Figura 4-6, en la interfaz física también son definidos otros tres parámetros: *CPThresh_* (*Capture Threshold*), *CSThresh_* (*Carrier Sense Threshold*) y *RXThresh_* (*Reception Threshold*). Estos tres valores son umbrales de potencia que ns-2 emplea para determinar la correcta recepción, o no, de un paquete recibido en la interfaz física, tal y como muestra la Figura 4-7.

Por un lado, ns-2 utiliza el umbral *CSThresh_* para determinar si un paquete es detectado o no por la interfaz (ver Figura 4-7). Si el nivel de potencia recibida es menor a dicho umbral, el paquete será descartado y no será visible por la capa MAC, ni siquiera aparecerá como recibido en la traza de salida. Por otro lado, el umbral *RXThresh_* permite decidir de manera determinista si un paquete ha sido recibido correctamente. Aquellos paquetes que se hayan recibido con una potencia superior a este umbral serán recibidos por la capa MAC sin ningún tipo de interferencias. Ahora bien, si el nivel de potencia se encuentra entre *CSThresh_* y *RXThresh_*, la capa MAC detecta el paquete, pero lo descartará por no tener la suficiente potencia como para ser decodificado correctamente. El último de los umbrales es utilizado en caso de que sean recibidos simultáneamente dos paquetes. Si el paquete que está siendo recibido se encuentra al menos *CPThresh_* dBs por encima del nivel de potencia del paquete interferente, y cumple la condición anterior de superar *RXThresh_*, el paquete será decodificado correctamente por la MAC, y el paquete interferente será descartado por colisión, siempre y cuando supere el nivel *CSThresh_*. En caso de que el paquete que está siendo recibido no supere en *CPThresh_* dBs al nivel de potencia del paquete interferente, ambos paquetes serán descartados.

```
Phy/WirelessPhy set CPThresh_ 10
Phy/WirelessPhy set CSThresh_ 1.0e-12
Phy/WirelessPhy set RXThresh_ 3.1623e-12
Phy/WirelessPhy set freq_ 5.9e+9  #; Frecuencia portadora
Phy/WirelessPhy set L_ 1.0        #; Constante de pérdidas
Phy/WirelessPhy set Pt_ val(pt)   #; Potencia de transmisión
Phy/WirelessPhy set Rb_ 6.0e6            #; Tasa de tx. de datos
```

Figura 4-6. Configuración de la interfaz física de los nodos móviles de ns-2



(a) Recepción de paquete. (b) Interferencias.

Figura 4-7. Esquema empleado por ns-2 para determinar la recepción de un paquete.

El esquema expuesto anteriormente, es el procedimiento que sigue la versión predeterminada de ns-2 para determinar la correcta recepción o no de un paquete. Sin embargo, en un caso más realista [27], un paquete recibido con una potencia *P* y un nivel de interferencia *I*, en algunos casos se recibirá correctamente y en otros no, debido a la naturaleza probabilística del ruido y de la propia interferencia. Es decir, la recepción de un paquete deberá determinarse de forma probabilística en función de la potencia de la señal recibida, el ruido y la interferencia (SINR, *Signal to Interference and Noise Ratio*). Esta probabilidad se expresa habitualmente en términos de tasa de error de bits (BER, *Bit Error Ratio*), de paquetes (PER, *Packet Error Ratio*) o de tramas (FER, *Frame Error Ratio*). El presente proyecto emplea curvas de PER para decidir de forma probabilística si un paquete es recibido correctamente. Dichas curvas fueron obtenidas en [28] considerando el estándar 802.11a. El modo de funcionamiento es el siguiente: a partir de un nivel de SINR, y dependiendo de la modulación asociada a dicho paquete, se obtiene su PER con la ayuda de las curvas de PER. Para decidir si el paquete es recibido o no

correctamente ya no nos vale únicamente que el nivel de señal recibida supere *CSThresh_*, ahora también se debe cumplir que el valor de PER obtenido sea menor que un número aleatorio (comprendido entre 0 y 1), que se genera al recibir el paquete. De este modo es como el descarte del paquete pasa a ser estocástico. Como podemos ver, el umbral *RXThresh_* pasa a estar en desuso.

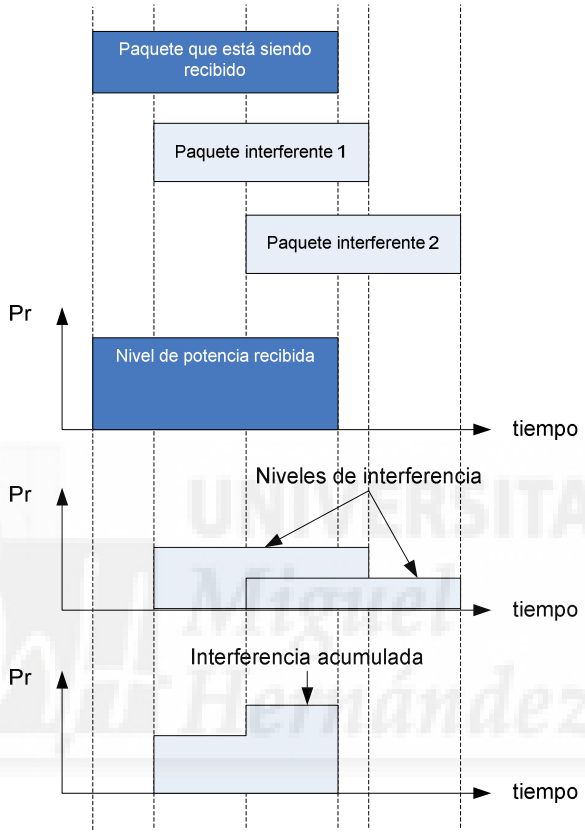


Figura 4-8. Cálculo de interferencia mejorado.

Otra modificación introducida en el simulador está relacionada con el cálculo de potencia de los paquetes interferentes. En la implementación por defecto de ns-2 sólo es considerado como interferente el paquete recibido de mayor potencia. Sin embargo, para el cálculo de interferencias debería tenerse en cuenta la suma de potencias de todos aquellos paquetes interferentes, considerando además el instante en el que son recibidos, la duración del interferente, etc. La Figura 4-8 ilustra un ejemplo, en el que se recibe un paquete, cuya potencia supera *CSThresh_* y empieza a ser procesado cuando se reciben otros dos paquetes. Como puede observarse, la influencia de los paquetes interferentes es acumulativa y sólo está presente durante la duración del paquete recibido.

La última modificación del simulador considerada en la presente tesis permite que, si en el momento que se está recibiendo un paquete, se recibe otro (interferente) cuyo nivel

de potencia es superior, este nuevo paquete pasa a ser el recibido y el anterior se verá como un interferente para el nuevo paquete.

4.2.3 Capa MAC 802.11 en ns-2

El bloque MAC/802_11 de ns-2 implementa todas las funcionalidades del protocolo IEEE 802.11 en su modalidad DCF, en la que no se emplean elementos de infraestructura para gestionar el acceso al canal radio. Se sigue la secuencia de envío RTS/CTS/DATOS/ACK para paquetes *unicast*, y realiza directamente el envío de DATOS en paquetes *broadcast*, *multicast* y en paquetes *unicast* de tamaño mayor a *RTSThreshold_*, tal y como indica el protocolo IEEE 802.11.

```
#802.11a
       Mac/802_11 set newchipset_           true
       Mac/802_11 set avgPER_               true
       Mac/802_11 set usePER_               true
       Mac/802_11 set SlotTime_             0.000009
       Mac/802_11 set SIFS_                 0.000016
       Mac/802_11 set PreambleLength_       120
       Mac/802_11 set PLCPHeaderLength_     24
       Mac/802_11 set PLCPDataRate_         6.0e6
       Mac/802_11 set dataRate_             6.0e6
       Mac/802_11 set basicRate_            6.0e6
       Mac/802_11 set RTSThreshold_         2346
       Mac/802_11 set ShortRetryLimit_      7
       Mac/802_11 set LongRetryLimit_       3
       Mac/802_11 set CWMin_                15
       Mac/802_11 set CWMax_                1023
       Mac/802_11 set aarf_                 true
```

Figura 4-9. Configuración de los parámetros MAC para IEEE 802.11a en ns-2.

Al igual que en los anteriores bloques, van a mostrarse aquellos parámetros que permiten ser configurados desde el *script* OTcl (Figura 4-9). La correcta configuración de estos valores es muy importante, pues cada uno de los estándares IEEE 802.11 se diferencia, entre otras cosas, en el valor que adquieren estos parámetros. Los valores mostrados corresponden a los valores empleados para la simulación del estándar IEEE 802.11a [18].

Basándonos en los parámetros de la Figura 4-9 se realizará una explicación de la implementación de la capa MAC en ns-2. Como se puede observar es posible configurar mediante código OTcl los valors *SlotTime_* y *SIFS_* que marcan el intervalo entre paquetes de datos en el canal. También se permite la configuración del tamaño de las cabeceras de los paquetes en bits (*PreambleLength y PLCPHeaderLength*); para obtener su equivalente en tiempo también se debe introducir la tasa de transmisión a la que son enviados (*PLCPDataRate_*). Se distinguen dos tasas de transmisión, una denominada *basicRate*, tasa a la que son enviados los paquetes de control (RTS, CTS y ACK), y la denominada *dataRate_* que es la tasa a la que son enviados los datos. Los valores de *ShortRetryLimit_* (límite para paquetes de tamaño menor a *RTSThreshold*) *y LongRetryLimit_* (en el caso de paquetes de tamaño superior a *RTSThreshold*) indican el número de retransmisiones permitidas hasta la recepción del ACK del receptor. Relacionado con el mecanismo de retransmisión se encuentran los valores de *CWMin_* y *CWMax_*, que hacen referencia a los valores mínimos y máximos permisibles para el cálculo del mecanismo de *backoff*.

Es importante realizar una puntualización adicional. Muchas de las técnicas de incentivo a cooperación basadas en reputación utilizan la técnica de observación *watchdog* para la vigilancia del comportamiento de los nodos vecinos. Como se dijo en la sección 2.3.1, esta técnica consiste en que cada nodo observa si los nodos vecinos retransmiten o no los paquetes que deben retransmitir. Para que esto sea posible, la MAC de los nodos que observan el comportamiento de los demás nodos debe funcionar en modo promiscuo. En este modo de funcionamiento, cada nodo escucha y procesa no solamente los paquetes que van dirigidos hacia él (en modo *unicast* o *multicast*), sino todos los paquetes que recibe en la interfaz física. De esta manera, analizando el contenido de los paquetes, el nodo puede evaluar si los nodos vecinos están retransmitiendo o no los paquetes que deben retransmitir, como se verá en la sección 5.2. Para configurar en modo promiscuo la MAC de los nodos en la implementación en ns-2 del estándar 802.11 utilizada en la herramienta de simulación, se han realizado algunas modificaciones en la implementación original. Los paquetes de datos que son recibidos correctamente en la interfaz física, son analizados para evaluar si deben ser encaminados hacia las capas superiores. En el caso de que sean paquetes *unicast* dirigidos a otros nodos, en la implementación original serían desechados. En cambio, en la implementación utilizada en la tesis, con la MAC en modo promiscuo, estos paquetes son marcados con la etiqueta *wachdog* y enviados hacia las capas superiores. Los paquetes marcados con la etiqueta *watchdog* son enviados hacia la técnica de reputación correspondiente para su procesamiento, tal como se describe en las secciones 5.3 y 5.4 en el siguiente capítulo.

4.3 Escenarios y parámetros de configuración

4.3.1 Patrones de tráfico de usuario

Con el objetivo de dar mayor realismo a las simulaciones realizadas, ns-2 permite incorporar al *script* OTcl distintos patrones de tráfico de datos. En [20] se pueden encontrar aportaciones de distintos grupos de trabajo relacionadas con estos patrones. El modelo de tráfico utilizado simula conexiones de descarga de tráfico web, extraído de las indicaciones en [29]. En [29] se especifican los valores que deben tomar los parámetros del modelo, que consiste en la descarga de páginas web por sesiones. En cada sesión, el usuario se descarga un número aleatorio de páginas web, que tienen un tamaño diferente, determinado por número de paquetes también aleatorio. El número promedio de páginas descargadas por sesión es de 5, mientras que el número promedio de paquetes por página web es de 25, y el tamaño promedio de cada paquete es de 366 bytes. También se define un tiempo medio de lectura tras la descarga de una página de 30 segundos. Al finalizar este intervalo de tiempo, se inicia la descarga de una nueva página. Los valores promedio de los parámetros se muestran en la Tabla 4-5.

Parámetro	Valor promedio
Número de páginas por sesión	5
Número de paquetes por página	25
Tamaño de paquete	366 bytes
Tiempo de lectura entre páginas	30s

Tabla 4-5. Valores promedio de los parámetros del modelo de tráfico web.

Cada uno de los nodos de la red establece conexiones multi-salto con un nodo situado en el punto medio del escenario. Para poder llevar a cabo un estudio del efecto de la congestión en la red se han considerado dos tipos de tráfico. En el primero, con sesiones no simultáneas, cada sesión se inicia después de que haya finalizado la sesión anterior. En el segundo tipo, con sesiones simultáneas, cada nodo inicia su sesión aunque el nodo anterior no haya finalizado la suya. El intervalo entre el inicio de la sesión de un nodo y el inicio de la sesión del nodo siguiente en sesiones simultáneas viene determinado por una variable aleatoria con distribución exponencial y media determinada por la Tabla 4-6. Los tiempos escogidos corresponden a una carga promedio en la red de un 15% de nodos activos transmitiendo cada momento. Para la elección del tiempo entre sesiones *tses* se ha empleado la siguiente fórmula:

$$tses = \frac{150}{nn * 0.15} \tag{4-6}$$

donde *nn* representa el número de nodos en la red, 150 representa el tiempo promedio de duración de las sesiones (el producto del número de páginas por sesión por el tiempo de lectura entre páginas, ver Tabla 4-5), y 0.15 corresponde al valor del 15% de conexiones activas. En el tráfico con sesiones no simultáneas, se evita el efecto de la congestión, para mostrar únicamente el efecto de las técnicas de cooperación, mientras que en el tráfico con sesiones simultáneas se podrá comprobar cómo afecta este la congestión al funcionamiento de dichas técnicas.

Número nodos	Tiempo entre sesiones [s]
114	8.7
238	4.2
406	2.4

Tabla 4-6. Tiempo entre sesiones promedio del modelo de tráfico web.

4.3.2 Topología del escenario

Las simulaciones realizadas en el presente trabajo han sido llevadas a cabo en diferentes escenarios y condiciones, tratando de emular las condiciones que pueden existir en una red de comunicaciones multi-salto. Se han considerado tres tamaños de escenario, que se hacen referencia al lado del cuadrado que lo delimita (900, 1350 y 1800 metros). Se ha escogido una topología de tipo Manhattan en el que los nodos se desplazan por calles rectangulares de 25 metros de anchura y que separan edificios cuadrados de 200 metros de lado. El punto central del escenario corresponde al punto de acceso al que se conectan los nodos para acceder al servicio de tráfico web. En cada uno de los tres tamaños de escenario varía el número de edificios considerados, 4, 6 y 8 respectivamente, en los cuales sin embargo se mantiene constante el valor de la densidad de nodos. El valor escogido para este parámetro, 1 nodo cada 80 metros aproximadamente, asegura que se establecen correctamente conexiones multi-salto. Para ajustarlo en cada escenario, se varía el número de nodos según el número de edificios, mediante la siguiente fórmula:

$$nn = \frac{225 \cdot nedif\,(nedif + 1) \cdot 2}{\lambda} \tag{4-7}$$

donde *nn* representa el número de nodos, *nedif* representa el número de edificios y λ representa la inversa de la densidad lineal de nodos λ=80 [m/número nodos]. Por ello, los valores escogidos son los que se muestran en la Tabla 4-7:

Número nodos	Dimensión [m]	Densidad [m/nodo]
114	900	78.9
238	1350	79.1
406	1800	79.8

Tabla 4-7. Número de nodos y dimensiones de los escenarios

Además del dimensionado del escenario, otro aspecto importante a determinar es la potencia de transmisión. Este parámetro influirá por un lado en el alcance de la transmisión, es decir, cuántos metros podrá recorrer el paquete en una transmisión de un solo salto, y por otro en la interferencia, ya que a mayor potencia de transmisión mayor interferencia se generará y mayor alcance tendrá. Teniendo en cuenta los valores de potencia de transmisión *Pt* de equipos WiFi comerciales convencionales, se han escogido dos niveles: *Pt = 0.05 W (17 dBm)* y *Pt = 0.1 W (20 dBm)*. El último valor estaría por encima de la media de los valores normales en equipos de usuario, pero dentro de los valores permitidos para puntos de acceso. Se podrán comparar los resultados obtenidos para ambos niveles de potencia, y apreciar el efecto de un mayor alcance, que reducirá el número de saltos en las transmisiones, y por tanto influirá notablemente en los valores de los parámetros finalistas.

4.3.3 Movilidad

Se ha utilizado un script implementado en Matlab [30] para generar archivos de movimiento que tengan en cuenta las características de movilidad de los peatones en entornos urbanos. El entorno urbano considerado corresponde a un escenario de tipo Manhattan o cuadrícula en el que todos los bloques de edificios son de igual tamaño y están distribuidos de forma regular. En este escenario, los nodos se desplazan siguiendo un modelo de movilidad "*Random Walk Obstacle*" [31]. Los peatones, que serán los nodos en la simulación, pueden realizar los siguientes movimientos:

- Desplazarse a una velocidad media de entre 2 y 3 m/s.
- Detener su movimiento durante un tiempo aleatorio.
- Girar en cualquiera de las direcciones al llegar a una intersección.

El *script* de Matlab genera una instrucción de movimiento cuando cada nodo llega a una intersección. En ella se indica la velocidad que el nodo debe mantener hasta alcanzar la siguiente intersección o hasta la siguiente parada. Estas instrucciones son generadas en un lenguaje directamente interpretable por ns-2. La Figura 4-10 muestra una disposición aleatoria de los nodos dentro del escenario Manhattan en el instante inicial. Las líneas

punteadas representan el centro de las calles por las que circulan los peatones. Estas calles poseen una anchura de 25m. Los espacios en blanco que quedan entre las calles representan los distintos edificios, que poseen unas dimensiones de 200m de lado. En los capítulos 5 y 6 el punto de acceso se sitúa en el centro del escenario (5000, 5000), mientras que en el capítulo 8, en donde el escenario corresponde a una red multi-salto celular, ese lugar es ocupado por la estación base.

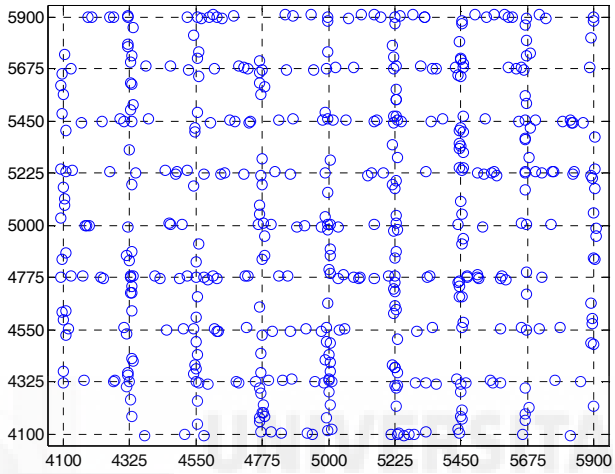


Figura 4-10. Representación de la posición inicial de los nodos en el escenario Manhattan.

4.3.4 Modelos de canal

Se han escogido tres modelos de canal diferentes para las simulaciones, a partir de los modelos de propagación discutidos en el apartado 4.2.1. El primero de ellos, al que nos referiremos como modelo 2 rayos, es el utilizado por defecto en el simulador ns-2 y el que emplean la inmensa mayoría de los estudios consultados (ver Tabla 2-6). Su empleo es sencillo pero sus predicciones son demasiado optimistas y no tienen en cuenta los efectos de la existencia o no de visibilidad directa entre emisor y receptor por los edificios que actúan como obstáculos y los efectos del canal radio (*shadowing* y *multipath fading*). El segundo modelo de canal empleado se corresponde con el el modelo de propagación micro-celular de entorno urbano publicado en [26], explicado en el apartado 4.2.1, y en adelante se denominará LOS-NLOS. Este modelo da cuenta de la existencia de visibilidad directa, al aplicar distintos valores para los parámetros del exponente del *pathloss* y de la desviación típica en función de si la transmisión se ve obstaculizada por un edificio. Este factor aporta un mayor realismo a la simulación y afecta considerablemente a los resultados obtenidos. Se ha estudiado además el efecto de un tercer modelo, denominado en adelante modelo realista, que además de la visibilidad tiene en cuenta el *shadowing* y el *multipath fading*, ya explicado en el apartado 4.2.

UNIVERSITAS
Miguel
Hernández

5

Dimensionado y viabilidad de técnicas de reputación en redes MANET

Los nodos de una red MANET pueden comunicarse entre ellos bien directamente (un salto o *single-hop*) o bien indirectamente (multi-salto o *multi-hop*). Además, los nodos en este tipo de redes suelen tener limitaciones en cuanto a batería, capacidad de procesamiento y comunicación. No requieren una entidad central de administración o una infraestructura de red fija pero precisamente por esto las principales funciones de red deben ser desempeñadas por los nodos de manera distribuida. Cuando se requiere establecer una conexión entre un par de nodos que no se encuentran en el rango de comunicación, la red se sirve de nodos intermedios para retransmitir los paquetes de datos. Sin embargo, dado que los nodos móviles están limitados por recursos como la energía y la capacidad de computación, algunos nodos pueden rehusar utilizar estos recursos para retransmitir paquetes que no son de su interés, aunque sí esperen por otro lado que otros nodos retransmitan sus paquetes [32]. En este contexto, es importante fomentar la cooperación de los nodos en el proceso de retransmisión [33], de manera que se asegure la conectividad y la viabilidad del conjunto de la red. Para tal cometido, en la literatura se han propuesto técnicas de incentivo a cooperación. Si bien existen distintas categorías de técnicas, esta tesis se centra en las basadas en reputación, en las que cada nodo de manera distribuida lleva a cabo una doble tarea: vigilancia del grado de

cooperación de los nodos de su entorno, y catalogación de los mismos en función de esas observaciones en categorías tales como nodos egoístas/cooperativos. Dicha información se emplea posteriormente durante los procesos de búsqueda y establecimiento de ruta para evitar y aislar a los nodos egoístas descubiertos y utilizar únicamente rutas seguras. Sin embargo, el éxito de estas técnicas depende en gran medida de la utilización de una técnica de observación fiable, capaz de distinguir de manera precisa las acciones egoístas que lleven a cabo los nodos vecinos. Aunque numerosos trabajos han evaluado el rendimiento de los sistemas basados en reputación, hasta ahora dicha evaluación no había empleado modelos de canal y condiciones de simulación realistas, con lo cual las conclusiones obtenidas podrían no ser fiables. El objetivo de este capítulo es pues evaluar el funcionamiento y rendimiento de las técnicas de reputación en base a la precisión en el modelado del canal radio con el fin de dar indicaciones sobre el rendimiento de este tipo de técnicas, y poder detectar deficiencias en su funcionamiento que puedan ser posteriormente corregidas.

5.1 Nodos no cooperativos en redes MANETs

No existe uniformidad en la nomenclatura ni en la tipología de los distintos tipos de nodo no cooperativo, es decir, en los distintos modelos de actuación de aquellos nodos que presentan alguna anomalía en su funcionamiento en cuanto al enrutamiento de paquetes de datos y señalización (ver sección 2.1.1). Diferentes estudios divergen en cuanto a cómo clasificar los distintos tipos de comportamientos no cooperativos (ver Tabla 2-1). Generalizando, estos comportamientos se pueden clasificar en tres tipos: nodos inactivos, nodos egoístas y nodos maliciosos. Los nodos inactivos son aquellos que no participan en ninguna tarea relacionada con la red, ni a nivel de datos ni a nivel de control. Su única influencia en la red podría ser aumentar o disminuir la densidad de nodos cooperativos (respecto al total de nodos), y por tanto no son de interés en esta tesis. Los nodos egoístas son aquellos que por alguna razón (escasez de recursos como la batería, la capacidad de computación o comunicación, configuraciones determinadas por el usuario, entre otras) participan en las tareas de enrutamiento, pero luego no retransmiten los paquetes que le son encomendados. Si bien existen otras posibles definiciones de nodo egoísta, coinciden en que el nodo no causa un daño intencionado a la red, sino que el daño provocado se deriva indirectamente del interés del nodo en preservar sus propios recursos. Por el contrario, los nodos maliciosos son aquellos que tienen la intencionalidad perjudicar en algún modo a la red de manera activa, afectando a los procesos de enrutamiento y corrompiendo o descartando paquetes, aún a costa de gastar sus propios recursos. Los ataques que pueden perpetrar los nodos maliciosos son muy variados (*black hole* o *grey hole*, *spoofing*, *denial of service*, suplantación de

identidad, etc.). Para contrarrestar la acción de los nodos maliciosos, se hace necesario implementar técnicas de seguridad específicas a cada tipo de ataque. En cuanto a los nodos egoístas, el efecto de su comportamiento sobre la conectividad de una red MANET ha sido estudiado ampliamente en la comunidad científica [37]. Los usuarios de la red perciben una reducción del rendimiento y de la calidad de servicio. A nivel de red, disminuye la conectividad de la red, hasta tal punto que pueden aparecer segmentos inconexos entre sí. La intensidad de esta reducción depende de distintos factores como el porcentaje de nodos egoístas en la red, su distribución, su grado de egoísmo, el tipo de acciones egoístas que se ejecutan, etc. Para contrarrestar estos efectos, es necesaria la aplicación de algún tipo de técnica de incentivo a cooperación. Estas técnicas tienen el objetivo de evitar que los nodos egoístas participen en la red, bien incentivándolos a cooperar, lo cual puede mejorar la conectividad global, o bien impidiendo que participen en la red, con lo cual se puede evitar al menos la reducción de conectividad que provoca su comportamiento. Sin embargo, detectar a los nodos egoístas o establecer técnicas para incentivarlos a cooperar es un reto que todavía no ha sido cerrado. Esta tesis doctoral se centra en los nodos egoístas cuyo comportamiento consiste en participar en las tareas de búsqueda y establecimiento de rutas (para no aislarse de la red) pero no en la retransmisión de paquetes para los demás [37]. Este tipo de nodo retransmite los mensajes de establecimiento de ruta establecidos en el protocolo de enrutamiento (RREQ *Route REQuest*, RREP *Route REPly*) pero, una vez establecida la ruta, no retransmite los paquetes que otros nodos le envían para su retransmisión, sino que los descarta. Como establece [38], un nodo puede descartar todos los paquetes que le llegan (asunción que será considerada en los capítulos 5 y 6 de este trabajo) o bien descartar sólo una parte de ellos (tal y como se asume en los capítulos 7 y 8).

La ausencia de una entidad central dificulta la vigilancia del comportamiento de los nodos, tal como se ha podido constatar en la literatura sobre MANETs [37], donde se han propuesto técnicas de incentivo a cooperación para fomentar la colaboración entre los nodos en las funciones de la red. Las técnicas se clasifican en distintas categorías, según la metodología aplicada para contrarrestar las consecuencias de las acciones de los nodos egoístas: basadas en reputación, basadas en crédito y basadas en teoría de juegos [37]. Por las razones expresadas en el capítulo 2, en este trabajo se estudian exclusivamente las técnicas basadas en reputación, en las que los nodos registran el comportamiento observado de los otros nodos (es decir, si retransmiten o no los paquetes). La técnica de observación más extendida es la técnica *watchdog* propuesta en [40]. En la literatura se han propuesto otras técnicas para la observación de la retransmisión de los paquetes por los nodos vecinos, como el esquema TWOACK [41], o los que consideran datos estadísticos de recepción de tramas en la capa de enlace de datos como en [42]. Frente a los inconvenientes de estos mecanismos, comentados en el capítulo 2, *watchdog* es el

método de observación estudiado en esta tesis. Constituye el mecanismo más referenciado en la literatura, introducido por primera vez en [40] y empleado entre otros en [43] y en [44]. En la técnica *watchdog*, cada nodo lanza un proceso de vigilancia con un temporizador para monitorizar las acciones de retransmisión de paquetes de sus nodos vecinos. Entre otros nuchos, [43] y [44] proponen reforzar la cooperación de los nodos, usando *watchdog* para identificar y aislar a los nodos egoístas.

Las técnicas de cooperación basadas en reputación que emplean la técnica de observación de *watchdog* son completamente distribuidas, tienen un buen rendimiento en términos generales y hacen un uso eficiente del canal de comunicación inalámbrico [37]. Sin embargo, en los estudios de la literatura sobre MANETs, la evaluación de estas técnicas fue realizada en condiciones de operación que podrían resultar demasiado simplistas, y por tanto, proporcionar indicaciones equívocas sobre su rendimiento y funcionamiento. En este capítulo se analizan distintas técnicas de incentivo a cooperación propuestas en la literatura que emplean la técnica *watchdog* como técnica de observación, y evalúa la influencia de importantes aspectos de modelado en el rendimiento y funcionamiento de las técnicas de cooperación en redes MANET. En particular, se investiga el impacto de considerar modelos de propagación radio precisos, y diferentes condiciones de congestión de canal y de funcionamiento, en el rendimiento de las técnicas de reputación, y en su capacidad para detectar correctamente a los nodos egoístas. Entender adecuadamente el impacto de estos factores en el funcionamiento de las técnicas de reputación es crucial para el perfeccionamiento de las mismas, y para la tarea de diseño de mejores técnicas, realizado en el capítulo 6. El objetivo es comprobar la influencia real de estos factores, que no han sido suficientemente tenidos en cuenta anteriormente, y dimensionar un escenario de red MANET en el cual desarrollar en capítulos posteriores técnicas que permitan solventar las posibles deficiencias en el rendimiento de la técnica *watchdog* al ser evaluado en condiciones realistas. Sin embargo, debe recalcarse que *watchdog* no puede evaluarse en solitario, sino como complemento a alguna técnica de incentivo a cooperación basada en reputación. De esta forma, puede evaluarse tanto el rendimiento de *watchdog* como su impacto sobre la técnica de reputación considerada y finalmente sobre la conectividad y el rendimiento de la red. Por tanto, en este trabajo se han seleccionado dos técnicas de cooperación basadas en reputación que emplean como técnica de observación el *watchdog*. Marti [40] fue el trabajo iniciador que propuso y empleó la técnica *watchdog* por primera vez, y ha sido implementada en esta tesis dada su sencillez como técnica de referencia con la cual comparar otras técnicas más recientes y avanzadas. Para ello se escogió TEAM [44], que refina el procedimiento del *watchdog* inicial mediante el uso de distintos tipos de reputación cuya influencia en el cómputo final de reputación es compensada por un coeficiente según la fiabilidad de la observación realizada. También se comparará el

rendimiento de estas dos técnicas con el de la red funcionando sin ninguna técnica de reputación, y con una técnica idealista, denominada PD (*Perfect Detection*), implementada como una cota superior de rendimiento a modo comparativo, cuya característica es que cada nodo conoce de antemano la identidad correcta de los nodos egoístas.

5.2 Técnica de observación *watchdog*

Las técnicas de reputación tienen como objetivo detectar y aislar a los nodos egoístas para incentivarlos a cooperar en las comunicaciones multi-salto. Se pueden dividir normalmente en dos módulos: monitorización y reacción. Cada nodo emplea su módulo de monitorización para observar si los nodos vecinos retransmiten o no paquetes de otros nodos. El módulo de reacción se encarga de actualizar la tabla de reputación en la que se asigna un nivel de reputación a los demás nodos con los que interacciona, a partir de las observaciones realizadas por el módulo de detección. Esta información puede ser usada después por los protocolos de enrutamiento para seleccionar la ruta más segura, libre de nodos egoístas. Además, los nodos egoístas pueden ser aislados de participar y establecer comunicaciones multi-salto. La mayoría de las técnicas de reputación emplean la técnica de observación *watchdog* [40]. Esta técnica se basa en una confirmación pasiva de la retransmisión de los paquetes por parte de los otros nodos, al vigilar el interfaz aire a la escucha de la retransmisión, tal y como refleja el ejemplo en la Figura 5-1. En lo sucesivo, el escenario representado en la Figura 5-1 será usado para explicar el funcionamiento de las técnicas de reputación y la técnica *watchdog*.

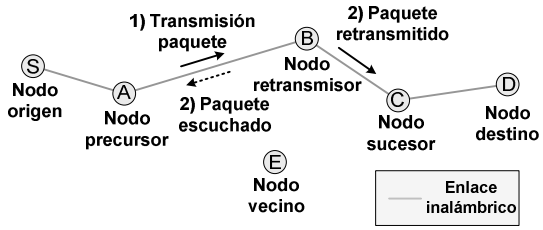


Figura 5-1. Funcionamiento del método de observación *watchdog*.

En el ejemplo mostrado en la Figura 5-1, el nodo origen (*S*) establece una ruta multi-salto para transmitir sus paquetes de datos hacia el nodo destino (*D*). En particular, los paquetes se transmiten desde el nodo origen siguiendo la secuencia *S, A, B, C* y *D*. En la Figura 5-1, un paquete está siendo transmitido desde el nodo *A*, que tiene el papel de nodo precursor (si se considera como nodo retransmisor al siguiente nodo), al nodo *B*, que tiene el papel de nodo retransmisor (paso 1 en la Figura 5-1). Un buffer de paquetes en el nodo precursor mantiene una copia temporal de los paquetes que deben ser retransmitidos por el nodo retransmisor. Cada paquete en el buffer tiene asignado un

Tiempo Límite dentro del cual el nodo precursor debe escuchar la retransmisión realizada por el nodo retransmisor. Si éste realiza la transmisión del paquete dentro del *Tiempo Límite* (paso 2), ésta es escuchada por el nodo precursor. Éste mirará en el buffer si existe alguna copia del paquete escuchado, y en tal caso borrará la copia y se registrará como la observación de una acción cooperativa, lo cual se denominará "observación de retransmisión de paquete". Si el nodo precursor no escucha correctamente la retransmisión del paquete dentro del *Tiempo Límite*, entonces se asume que el nodo retransmisor ha actuado egoístamente, es decir, que ha descartado el paquete. De manera análoga, este caso será denominado "observación de descarte de paquete". Este descarte se registra y se comunica al módulo de reacción de la técnica de reputación, que puede degradar la reputación del nodo en la tabla de reputación según sus propias indicaciones de la técnica de reputación correspondiente. Dependiendo de cómo se realice la observación, se pueden distinguir dos tipos de reputación: directa e indirecta. La reputación directa corresponde al caso ya explicado, donde es el nodo precursor el que observa el comportamiento del nodo retransmisor. Alternativamente, en la Figura 5-1, un nodo vecino *E* puede indirectamente observar la retransmisión del paquete desde el nodo precursor hasta el nodo retransmisor, y de allí hacia el nodo sucesor. En este caso, la observación de retransmisión de paquete se computaría como reputación indirecta. Sin embargo, este tipo de reputación resulta menos fiable al requerir no sólo que los nodos precursor y retransmisor tengan un enlace directo, sino también que ambos estén en el rango directo de comunicación del nodo vecino observador, lo cual no siempre será posible debido a la propagación radio.

El *Tiempo Límite* es el tiempo dentro del cual el nodo retransmisor debe retransmitir el paquete que ha recibido de otro nodo. En este contexto, el tiempo de observación de retransmisión se refiere al intervalo entre el instante en el cual la copia del paquete es almacenada en el buffer del nodo precursor, y el instante en el que es correctamente escuchada y borrada del buffer. El tiempo de observación de retransmisión incluye la suma de los retardos introducidos durante la transmisión del paquete desde el nodo precursor al nodo retransmisor y la retransmisión por parte de éste. Los paquetes se escuchan correctamente sólo cuando el *Tiempo Límite* es mayor que el tiempo de observación de retransmisión. Un valor demasiado alto del *Tiempo Límite* incrementa el tiempo necesario para detectar a los nodos egoístas, mientras que un valor demasiado bajo puede impedir que la retransmisión sea escuchada correctamente, incrementando la inexactitud del proceso de detección de nodos egoístas. Sin embargo, en la literatura no se ha encontrado una indicación definitiva sobre el valor al que debería ser fijado. El trabajo presentado en [45] implementa un banco de pruebas para analizar la técnica de observación *watchdog*, donde constata que en general el tiempo real para escuchar correctamente las retransmisiones de los paquetes estaba por debajo de 10ms, incluso en

el caso de una carga de tráfico alta. En el mismo trabajo, se fija finalmente el valor del *Tiempo Límite* a 100ms. Para encontrar un balance adecuado entre ambos extremos para el parámetro de *Tiempo Límite*, se llevaron a cabo simulaciones preliminares. Las simulaciones realizadas usaron la plataforma descrita en el capítulo 4 y consideraron que todos los nodos cooperaban en la retransmisión de paquetes. La Figura 5-2 representa la CDF (*Cummulative Distribution Function*) del tiempo de observación de retransmisión. La CDF representa la probabilidad de que en un porcentaje determinado de ocasiones se haya registrado un tiempo de observación de retransmisión menor que el indicado en el eje de abcisas. Para asegurar que la mayoría de los paquetes retransmitidos pueden ser escuchados correctamente, el *Tiempo Límite* seleccionado es mayor que el percentil 99 del tiempo de observación de retransmisión (igual a 41.5ms). En particular, el *Tiempo Límite* se ha fijado a 50ms.

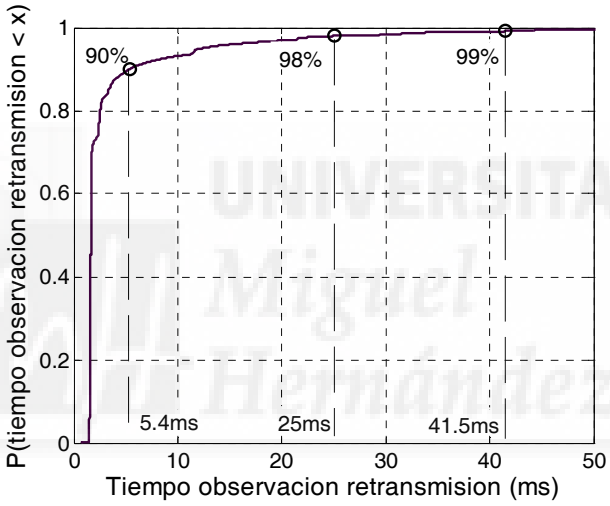


Figura 5-2. Distribución del tiempo de observación de la retransmisión.

La mayoría de técnicas de reputación de la literatura utilizan la técnica *watchdog*. Sin embargo, los errores de propagación radio y las colisiones de paquetes debido a la congestión del canal pueden deteriorar el rendimiento y la capacidad de detección del egoísmo de la técnica *watchdog* [46]. En el ejemplo ilustrado en la Figura 5-1, las colisiones de paquetes podrían impedir que el nodo precursor observara correctamente la retransmisión del paquete del nodo retransmisor. En [45] se afirma que las colisiones de paquetes no afectan a la capacidad de detección de *watchdog*, incluso en un entorno con una gran carga de tráfico. Sin embargo, el escenario de evaluación de dicho trabajo podría ser demasiado limitado al estar formado por un banco de pruebas de 4 nodos. Las observaciones de descartes incorrectas repetidas que afectan a un nodo pueden conducir a su acusación incorrecta, lo cual puede impedir que participe en las comunicaciones multi-salto siguientes. Por tanto, puede verse reducida la disponibilidad de las denominadas rutas seguras, es decir, rutas sin nodos egoístas conocidos. Otro problema que puede

afectar a la capacidad de observación está relacionado con las caídas de enlace. La capa MAC en 802.11 dispone de un mecanismo para detectar las caídas de enlace y se encarga de iniciar un evento para informar al protocolo de enrutamiento. El protocolo de enrutamiento informa a su vez a la técnica de reputación correspondiente, que detiene el proceso de *watchdog* que vigila las retransmisiones del nodo retransmisor. Es posible entonces que en el buffer de *watchdog* exista todavía algún paquete cuya escucha de retransmisión está todavía pendiente. En esta implementación del *watchdog*, los paquetes en el buffer pendientes de retransmisión tras una caída de enlace no son contabilizados como "observación de descarte", es decir, como acciones egoístas, ya que no lo es propiamente y además ello podría aumentar injustamente el número de acusaciones incorrectas a nodos cooperativos. En su lugar, se ha optado por no contabilizar estas observaciones en las técnicas de reputación. Es decir, no se aumentará la cuenta de descartes o de retransmisiones que registran. Sin embargo, sí que se tendrá en cuenta en las estadísticas sobre el rendimiento de *watchdog* donde, en el caso de que sea realmente un nodo egoísta, contabilizarán como observaciones de descarte no realizadas.

5.3 Técnica de Marti

Como se comentó en el apartado 2.3, la primera técnica implementada en este trabajo fue propuesto en [40] y será denominado en lo sucesivo la técnica de Marti. En la técnica de Marti, cada nodo precursor utiliza la técnica de observación *watchdog* para observar el comportamiento de los nodos retransmisores. Cada nodo mantiene una tabla de reputación donde registra el nivel de reputación y el número de faltas de todos los nodos conocidos (aquellos con los que ya ha interaccionado anteriormente), a partir de la información compilada por la técnica *watchdog*. A su vez, durante los procesos de búsqueda y selección de ruta, se escoge aquella que tenga mayor probabilidad de ser segura, es decir, sin nodos egoístas conocidos, mediante un algoritmo heurístico, explicado a continuación.

Cada nodo cuenta el número de veces que un nodo retransmisor ha rechazado retransmitir sus paquetes. Cuando el número de faltas es mayor que un determinado umbral, que se denomina *Umbral Máximo de Faltas*, el nodo retransmisor es acusado de actuar egoístamente. La acusación se mantiene durante un período de tiempo denominado *Tiempo de Aislamiento*, tras el cual el nivel de reputación del nodo y su número de faltas vuelven a restaurarse en la tabla de reputación al nivel por defecto (*Reputación Inicial*) asignado a un nodo conocido por primera vez. La Tabla 5-1 muestra los valores de los parámetros de implementación de la técnica de Marti empleados en la presente

implementación[27], y el criterio aplicado para seleccionar dicho valor. El parámetro de *Tiempo de Aislamiento* no está especificado en la implementación original de Marti [40]. El Tiempo de Aislamiento se ha fijado a 500s, un valor superior a la duración media de la sesión de tráfico de usuario (151s en el modelo implementado). El *Tiempo de Aislamiento* definido asegura que las técnicas son suficientemente probadas durante el tiempo de simulación. Además, en la tabla de reputación cada nodo tiene asignado también un nivel de reputación, que se actualiza a partir de las observaciones realizadas por el módulo de monitorización, conforme a la siguiente heurística. El nivel de reputación de un nodo con el que se interacciona por primera vez comienza en el nivel *Reputación Inicial*. El nivel de reputación de todos los nodos que participan en una ruta activa se incrementa en cierto valor (*Incremento de Reputación*) cada cierto intervalo de tiempo (*Intervalo de Incremento de Reputación*). Marti define una ruta activa como aquella en la que ha habido actividad (envío o recepción de paquetes) en el último *Intervalo de Incremento de Reputación*. Por otro lado, el nivel de reputación del nodo se penaliza en un valor *Decremento de Reputación* cuando el *watchdog* del nodo precursor detecta una falta. El nivel de reputación de un nodo que no ha sido acusado permanece siempre en el rango [0.0,1.0]. Si un nodo es acusado de actuar egoístamente, su nivel de reputación se degrada a un valor muy negativo (*Reputación de Nodo Egoísta*).

Parámetro	Valor	Criterio
Reputación Inicial	0.5	Implementación original [40]
Tiempo de Aislamiento [s]	500	De acuerdo a modelo de tráfico
Umbral Máximo de Faltas	5	Análisis de trazas de simulación
Reputación nodo cooperativo	0.0 – 1.0	Implementación original [40]
Incremento de Reputación	0.01	Implementación original [40]
Intervalo de Incremento de Reputación (ms)	200	Implementación original [40]
Decremento de Reputación	-0.05	Implementación original [40]
Reputación de Nodo Egoísta	-100	Implementación original [40]

Tabla 5-1 Parámetros de configuración de la técnica de Marti.

El *Umbral Máximo de Faltas* no se especificaba en la implementación original de Marti [40], y por tanto el valor utilizado en este trabajo ha sido seleccionado tratando de balancear el compromiso existente entre la velocidad y la precisión del proceso de detección de los nodos egoístas [138]. Un valor muy grande incrementaría el número de

[27] Si no se especifica lo contrario, los valores numéricos de los parámetros de implementación se escogen de acuerdo a las indicaciones de la implementación original del protocolo de Marti [40] (ver Tabla 5-1).

paquetes que los nodos que actúan egoístamente descartan antes de ser acusados. Por otro lado, un valor demasiado reducido incrementaría el número de veces que los nodos cooperativos podrían ser acusados incorrectamente, por ejemplo debido a colisiones de paquetes o a errores de transmisión radio. En este contexto, se llevaron a cabo simulaciones preliminares con diferentes valores del parámetro *Umbral Máximo de Faltas* para poder seleccionar su valor óptimo, usando la plataforma y las condiciones de simulación especificadas en el capítulo 4. El resultado de dicha simulación se muestra en la Tabla 5-2 en términos de PDR[28] (*Packet Delivery Ratio*). El máximo PDR para los nodos cooperativos se alcanza con un *Umbral Máximo* de 5, que al mismo tiempo también garantiza el mínimo PDR para los nodos egoístas. Este efecto es deseable pues incentiva a los nodos a participar en la red retransmitiendo los paquetes de otros nodos.

Umbral Máximo	Nodos cooperativos	Nodos egoístas	Incremento [%] (coop./egoístas)
3	56.39	51.25	5.14
5	59.58	41.67	17.91
10	56.25	49.17	7.08
15	50.42	51.25	-0.83
20	52.08	47.08	5.00

Tabla 5-2 PDR de nodos egoístas y cooperativos.

La técnica de Marti también introduce mensajes de acusación que permiten al nodo precursor avisar al nodo origen (ver Figura 5-1) sobre la presencia de un nodo egoísta en la ruta. Sin embargo, debe tenerse en cuenta que estos mensajes podrían ser manipulados por nodos maliciosos y además pueden incrementar la carga de señalización. Para establecer un enlace multi-salto, el protocolo de enrutamiento intenta seleccionar una ruta sin nodos egoístas. Esto se consigue calculando la métrica *Reputación de Ruta*, que consiste en el promedio de la reputación de todos los nodos que participan en la ruta multi-salto. Los nodos egoístas tienen un valor de reputación muy negativo, y por tanto, cuando aparecen en alguna ruta, su *Reputación de Ruta* es negativa. Aquellas rutas con una *Reputación de Ruta* negativa son automáticamente rechazadas. Al seleccionarse la ruta con una mayor reputación, se reduce la probabilidad de participación de los nodos egoístas. También se rechazan las peticiones de búsqueda de ruta que provienen de nodos egoístas conocidos.

[28] El PDR o tasa de entrega de paquetes es una métrica de rendimiento que se calcula como el cociente porcentual entre el número de paquetes transmitidos en la red y el número de paquetes que han sido recibidos en el nodo destino correctamente.

5.4 Técnica TEAM

La segunda técnica de reputación implementada es la técnica TEAM (*Trust Enhanced security Architecture for Mobile ad-hoc networks*) [44]. TEAM ha sido seleccionada por ser una contribución más reciente y sofisticada que el protocolo de Marti [40]. TEAM propone tres tipos de reputación distintos, que se promedian por unos coeficientes para formar un valor de confianza para cada nodo. Además, entre estos tipos introduce un nuevo concepto de reputación, el de reputación recomendada, basada tanto en la actividad de los nodos retransmisores como en la reputación previa que tienen esos nodos en la tabla de reputación. Además, durante los procesos de búsqueda de ruta y de retransmisión de paquetes, TEAM es más estricta que Marti, al requerir la evaluación de distintos tipos de niveles de confianza según la entidad considerada: confianza de nodo, de ruta y de paquete.

TEAM distingue entre confianza y reputación. La reputación es la información de entrada a partir de la cual se calcula la confianza, que es el grado de cooperación demostrado por ese nodo en las observaciones previas realizadas, y la confianza en que sea un nodo fiable. La técnica se compone de dos módulos: monitorización y reacción. El módulo de monitorización usa tres tipos distintos de información de entrada para decidir si un nodo está o no actuando de manera egoísta: reputación directa, reputación indirecta (ambas usando la técnica de observación *watchdog*), y reputación recomendada. La confianza de un nodo es la suma ponderada por coeficientes de los tres tipos de reputación[29], como se muestra en la ecuación 5-1:

$$T_N^i(t_{a+1}) = \sum U^{tipo} \cdot \varpi_{N-i}^{tipo}(t_a), \tag{5-1}$$

donde $\sum U^{tipo} = 1$, $tipo \in \{directa, indirecta, recomendada\}$, $T_N^i(t_{a+1})$ es el nuevo nivel de confianza del nodo *i* en la tabla del nodo *N*, $\varpi_{N-i}^{type}(t_a)$ es el nivel de reputación del tipo del nodo *i* en la tabla del nodo *N*, y U^{type} es el coeficiente de cada tipo de reputación. Los coeficientes asignados a cada tipo de reputación no son uniformes, ya que la reputación directa es más fiable que las otras dos. Su valor en la presente implementación, mostrado en la Tabla 5-3, ha sido seleccionado siguiendo las indicaciones de distintos trabajos sobre TEAM [44][47]. En ninguno de estos trabajos se proporciona un valor exacto para los coeficientes, pero sí se especifica en [47] que el peso de la reputación directa debe ser mayor. Cuando un nodo aparece por primera vez en la tabla de reputación, generalmente durante el proceso de búsqueda y establecimiento de ruta, se inicializan los tres tipos de

[29] Salvo que se especifique lo contrario, y siempre que ha sido posible, los valores escogidos para los parámetros de TEAM en la presente implementación han sido los mismos que los especificados en la implementación original [44][47].

reputación al valor por defecto Δ o *umbral mínimo*. Los niveles de reputación directa e indirecta de un nodo en la tabla de reputación se incrementan o disminuyen en cierto nivel (*Incremento de Reputación* / *Penalización de Reputación*, ver Tabla 5-3) tras la observación de una retransmisión correcta o de un descarte de paquete por parte del nodo. Además, cuando un nodo recibe un paquete que debe ser retransmitido, la reputación recomendada de los nodos que han retransmitido previamente el paquete se actualiza, asumiendo que, si un nodo retransmite un paquete proveniente de otro nodo, es porque lo recomienda implícitamente (en definitiva, considera que no es un nodo egoísta). Tomando como ejemplo la Figura 5-1, en donde la transmisión del paquete desde el origen al destino sigue la secuencia de saltos entre los nodos *S*-*A*-*B*-*C*-*D*, cuando el paquete llega al nodo *C*, este puede deducir una reputación recomendada del nodo *A*. Los papeles de cada nodo en este caso serían los siguientes: *A* nodo recomendado, *B* nodo que recomienda, y *C* nodo que recibe la recomendación. La reputación recomendada del nodo *A* en la tabla del nodo *C* se ajusta aumentándola en un cierto valor fijo. Este valor es ponderado por un factor multiplicador, que es la confianza que el nodo *C* tiene en el nodo que recomienda, *B*. Esta ponderación se realiza porque *B* es el nodo que recomienda, y por tanto debe tenerse en cuenta cómo de fiable es su recomendación en la opinión del nodo *C* que la recibe. Se pueden encontrar más detalles sobre la reputación recomendada en [44]. Si el nivel de confianza, calculado según la expresión (5-1), es inferior al *umbral mínimo* o Δ, entonces el nodo retransmisor es acusado de actuar egoístamente durante un período de tiempo igual al *Tiempo de Aislamiento* (elegido con el mismo criterio que en el apartado 5.3 para el protocolo de Marti y mostrado en la Tabla 5-2).

El módulo de reacción de la técnica TEAM se encarga de realizar las siguientes comprobaciones: confianza de nodo, confianza de paquete y confianza de ruta. El cálculo de la confianza para un nodo ha sido explicado (expresión 5-1). La comprobación de la confianza de paquete debe hacerse cuando un nodo intermedio recibe un paquete que debe retransmitir. Consiste en evaluar la confianza de ciertos nodos de la ruta que atraviesa el paquete: el nodo origen, el nodo destino, el nodo precursor y el nodo sucesor (ver Figura 5-1). Sólo se accede a la retransmisión si la confianza de cada uno de estos nodos es mayor que el *umbral mínimo* Δ. Además, cuando un nodo recibe un mensaje de petición de ruta (RREQ) o un mensaje de confirmación de ruta (RREP), para establecer una nueva ruta, el módulo de reacción acepta la petición sólo si la confianza de la ruta es mayor que Δ. La confianza de la ruta corresponde al promedio del valor de la confianza de todos los nodos que participan en la ruta. La Tabla 5-3 reúne los parámetros de TEAM, así como su valor en la presente implementación y la justificación de la elección de los valores. Como criterio de selección principal, se ha escogido el valor de la implementación original siempre que fuera posible. En otro caso, se han seguido las indicaciones existentes.

Parámetro	Valor	Criterio de selección
Coeficiente Reputación Directa U^D	0.75	Según indicaciones implementación original[30]
Coeficiente Reputación Indirecta U^I	0.15	Según indicaciones implementación original
Coeficiente Reputación Recomendada U^R	0.15	Según indicaciones implementación original
Umbral Mínimo Δ	0.5	Implementación original [41]
Incremento Reputación	0.02	Implementación original [41]
Penzalización Reputación	-0.1	Implementación original [41]
Rango de Reputación	-1.0 – 1.0	Implementación original [41]
Tiempo de Aislamiento [s]	500	Asegurar la validación de la técnica

Tabla 5-3 Parámetros de configuración del protocolo TEAM.

5.5 Evaluación en condiciones realistas

Como se ha explicado anteriormente, el objetivo del capítulo es el estudio del rendimiento y funcionamiento de técnicas de cooperación bajo condiciones de modelado y funcionamiento realistas. Este estudio permitirá evaluar su capacidad para detectar nodos egoístas y fomentar una adecuada conectividad en redes MANET, así como detectar posibles deficiencias que se buscará corregir en capítulos posteriores.

5.5.1 Métricas de evaluación de rendimiento

La conectividad en una red MANET con presencia de nodos egoístas puede verse afectada por ciertos factores tales como el número de nodos egoístas, las condiciones de propagación radio o incluso la potencia de transmisión de los nodos. En este contexto, la Figura 5-3 resume las líneas de estudio que se han seguido en este capítulo, y que serán discutidas en detalle en este apartado. En la parte izquierda de la Figura 5-3 se muestran diferentes parámetros con repercusión sobre la conectividad de la red: el porcentaje de nodos egoístas, el protocolo de prevención de egoísmo, la potencia de transmisión, el modelo de propagación, el tamaño del escenario, y el efecto de la congestión. Se resume además la influencia de estos parámetros de entrada sobre algunos importantes factores del rendimiento de la red, como la conectividad, el porcentaje de detecciones falsas de la técnica de cooperación, la consideración de valores específicos para los parámetros de propagación en condiciones de no visibilidad por parte del modelo de canal, la distancia

[30] Cuando el valor exacto del parámetro se podía encontrar en la referencia correspondiente, se utiliza el criterio "Implementación original", mientras que cuando no es posible se aplica "Según indicaciones implementación original".

de salto, la distancia total entre emisor y receptor, y el número de saltos por transmisión. Los estudios realizados muestran que estos parámetros y factores están relacionados unos con otros. Para mostrar estas relaciones, se han empleado los signos "+" y "–". El signo "+" indica una relación directa, mientras que el signo "–" indica una relación inversa. Por ejemplo, si se incrementa el porcentaje de nodos egoístas, habrá más detecciones pero también menos conectividad, o si se aumenta la potencia de transmisión, aumentará la distancia de salto.

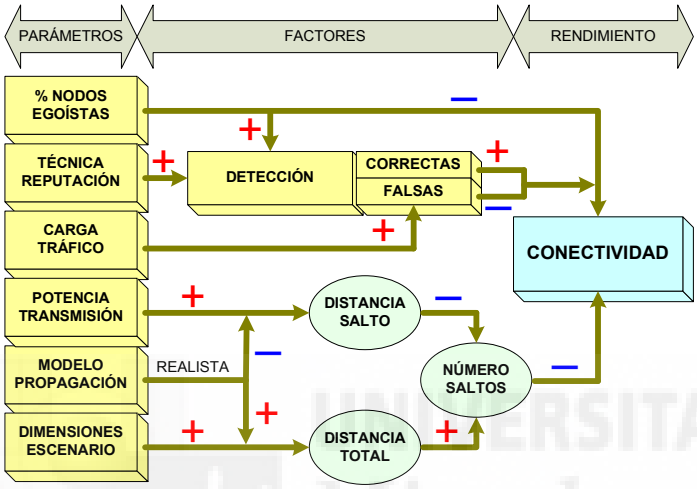


Figura 5-3. Parámetros y factores que influyen en la conectividad de la red en presencia de nodos egoístas.

Uno de los principales factores que afecta a la conectividad es el número de saltos entre el origen y el destino, el cual además también se ve afectado a su vez por la potencia de transmisión, la propagación radio y la densidad de nodos egoístas. Tal como muestra la Figura 5-3, cuanto mayor es el número de saltos entre el origen y el destino, mayor es la probabilidad de que la ruta que se establezca incluya un nodo egoísta. Para apreciar esto se muestran en la Figura 5-4 varias curvas que relacionan el número de saltos de la ruta con la probabilidad de encontrar un nodo egoísta en la misma, para distintos porcentajes de nodos egoístas. Incluso para un número de saltos bajo como 2 o 3 y un porcentaje de nodos egoístas de sólo el 20%, la probabilidad de encontrar una ruta sin nodos egoístas se reduce considerablemente. La Figura 5-4 se ha elaborado a partir de la expresión (5-2), en la que *P* representa la probabilidad de encontrar una ruta con algún nodo egoísta, *ns* es el número de saltos, *nn* el número de nodos, y *pns1* la fracción de nodos egoístas. Se asume que no se considera ninguna técnica de reputación en el proceso de selección de ruta, es decir, todas las rutas potenciales tienen la misma probabilidad de ser seleccionadas, independientemente del número de nodos egoístas que contengan. Esto quiere decir que la existencia de nodos egoístas junto con una técnica de reputación

incapaz de detectarlos correctamente puede afectar muy severamente a la conectividad de la red. El número de nodos asumido en la Figura 5-4 es de 238 (ver Tabla 4-7).

$$P = 1 - \prod_{i=1\ldots ns} \frac{\lfloor nn(1 - pns1) \rfloor - i + 1}{nn - i + 1} \tag{5-2}$$

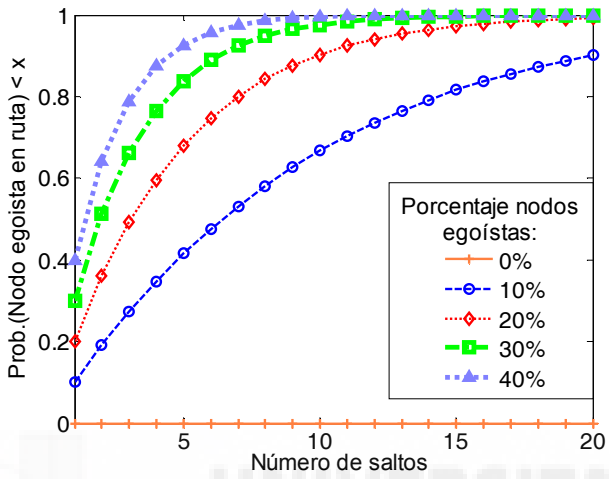


Figura 5-4. Distribución de la probabilidad de escoger aleatoriamente una ruta con nodos egoístas

En cuanto a las métricas que serán utilizadas para evaluar las técnicas de reputación, la Figura 5-3 refleja aquellos aspectos que deben ser examinados: por un lado, la tasa de entrega de paquetes o PDR, como parámetro de rendimiento final más importante. El PDR refleja de forma explícita y directa el efecto sobre la conectividad del resto de factores. Acompañando al PDR, se estudiarán también el porcentaje de paquetes no entregados por distintas causas: paquetes perdidos por la no disponibilidad de rutas o por caídas de enlaces, paquetes descartados por nodos egoístas, y paquetes descartados por su procedencia sospechosa (nodo origen egoísta o presencia de nodos intermedios egoístas en la ruta). Esta última categoría sólo se aplica en la técnica TEAM, ya que en la de Marti no se evalúan individualmente los paquetes para detectar aquellos que pudieran provenir de nodos egoístas.

La capacidad de las técnicas de reputación para detectar nodos egoístas, y la probabilidad de acusar incorrectamente a un nodo no egoísta, puede tener un impacto significativo sobre la conectividad y la probabilidad de establecer una ruta multi-salto segura desde el origen al destino. Por consiguiente, se proponen los siguientes parámetros de detección para cuantificar su capacidad de detectar a los nodos egoístas: el índice de sensibilidad positivo S^+ y el índice de error positivo E^+. El índice de sensibilidad positivo S^+ se define aquí como el cociente entre el número de observaciones correctas de descarte de paquete y el número total de paquetes que los nodos egoístas debían haber retransmitido. Por observaciones correctas de descarte de paquete se entiende aquellas

observaciones de descarte en las que el nodo retransmisor era efectivamente egoísta y realizó el descarte observado por el nodo precursor. En contraposición a esto, las observaciones incorrectas de descarte se refieren a aquellas observaciones de descarte en las que en realidad el nodo retransmisor era un nodo cooperativo, y por tanto están provocadas por errores de transmisión radio y colisiones de paquetes. Análogamente, el índice de error positivo E^+ se define como el cociente entre el número de observaciones de descarte incorrectas y el número de veces que se requiere que un nodo cooperativo retransmita un paquete. La eficiencia de la técnica de reputación se puede medir con el compromiso que hay entre ambos parámetros: la técnica más eficiente es la que obtiene una mayor sensibilidad S^+, sin incrementar como contrapartida el error E^+. Otro parámetro muy importante relacionado con el error positivo E^+ es el porcentaje de acusaciones falsas, que se define como el cociente entre el número de acusaciones falsas partido por el total de acusaciones realizadas. Aunque están relacionados, ambos parámetros no son equivalentes. Un número alto de observaciones de descarte incorrectas, relacionadas con el parámetro E^+, no siempre desembocan en acusaciones incorrectas, ya que las observaciones pueden estar realizadas por distintos nodos y que en ninguno de ellos se cumpla la condición de acusación de la correspondiente técnica de reputación. Esto se verá más claramente en los resultados que serán mostrados más adelante.

5.5.2 Plataforma y escenarios de evaluación

El estudio realizado en el presente capítulo ha sido llevado a cabo a través de simulaciones a nivel de sistema que emulan el funcionamiento de una red MANET empleando la plataforma de simulación ns-2 (*Network Simulator* v.2) presentada en el capítulo 4. En este contexto, el estudio se centra en un escenario urbano con diferentes niveles de congestión de tráfico y distintos modelos de canal radio con características de precisión diferentes. También es importante modelar adecuadamente los protocolos de comunicación *ad-hoc* multi-salto sobre los cuales se apoyan las técnicas de cooperación. Este estudio adopta el protocolo DYMO (sucesor del protocolo AODV) como protocolo de enrutamiento. Para más información sobre el protocolo de enrutamiento utilizado, consúltese el apartado 3.5.

La plataforma y las condiciones de simulación fueron presentadas de manera general en el capítulo 4. El escenario de simulación es de tipo Manhattan con un número variable de dimensiones (900x900m^2, 1350x1350m^2 y 1800x1800m^2, con número de nodos 114, 238 y 406 respectivamente). Las dimensiones y el número de nodos aseguran una densidad media de nodos suficiente para permitir el establecimiento de comunicaciones multi-salto (un nodo cada 80 metros a lo largo de las calles aproximadamente). En este escenario, los nodos se desplazan siguiendo un modelo de movilidad "*Random Walk*

Obstacle" [31]. La existencia de edificios no sólo restringe el movimiento de los nodos a determinadas direcciones, sino que además, influirá notablemente en el desempeño del sistema cuando se empleen modelos de canal que tengan en cuenta las condiciones de visibilidad reales y su efecto en la propagación de la señal. La tecnología de acceso radio empleada por los nodos es 802.11a a 5.8GHz, con una potencia de transmisión de 17dBm y 20dBm, utilizando una velocidad de transmisión de datos de 12 Mbps. Este valor representa un compromiso entre la velocidad de transmisión de datos y la robustez de la modulación frente a los errores de propagación radio (ver Tabla 3-1). El modelo de tráfico simula conexiones de descarga de tráfico web, extraído de las indicaciones en [29] (ver sección 4.3.1). Dado que el efecto de negativo de la congestión sobre la técnica de detección *watchdog*, señalado en [46], es motivo de controversia en [45], se han realizado dos tipos de simulaciones en cuanto al tráfico para estudiar el efecto de la congestión por separado. En el primero se evita el efecto de la congestión ya que cada nodo inicia su sesión cuando el anterior ha terminado la suya, en sesiones no simultáneas. En el segundo tipo de tráfico, con sesiones simultáneas, diferentes nodos pueden iniciar sus sesiones aunque otros nodos tengan sesiones en curso.

En cuanto a los modelos de canal, se emplean tres modelos distintos, con distintas precisiones en el modelado de las características del canal radio. Estos modelos de canal ya fueron presentados de manera más detallada en el capítulo 4. El modelo más simple es el de 2 rayos, que predice las mismas pérdidas que el modelo de espacio libre hasta cierta distancia crítica, a partir de la cual, las pérdidas tienen una dependencia de orden cuatro con la distancia (d^4). Frente a este modelo que no tiene en cuenta las condiciones reales de visibilidad entre emisor y receptor, este trabajo incluye otro más realista extraído del modelo urbano micro-celular desarrollado en el proyecto europeo WINNER [26]. Este modelo es uno de los más completos para entornos urbanos, con reducidas alturas de la antena de las estaciones, y que sí tiene en cuenta la diferencia entre condiciones de visión directa (LOS – *Line-of-Sight*) y no visión directa (NLOS - *Non Line-of-Sight*) y por ello se denominará LOS-NLOS. El tercero de los modelos es similar al LOS-NLOS pero además tiene en cuenta los siguientes efectos del canal radio: la correlación espacial del desvanecimiento lento y las perturbaciones provocadas por el desvanecimiento multitrayecto sobre el nivel de potencia recibida. Dichos efectos ya han sido descritos en el apartado 4.2. Este tercer modelo se denominará en lo sucesivo modelo Realista. La principal diferencia entre los dos últimos y el primero, además de tener un menor alcance, es que los últimos consideran las condiciones de visibilidad entre emisor y receptor, lo cual conlleva que las distancias recorridas por los paquetes sean en promedio mayores, y por tanto, las rutas estén compuestas por un número mayor de saltos, factor que degrada considerablemente el funcionamiento de la red en presencia de nodos egoístas como se verá.

La Tabla 5-4 resume los valores de los parámetros de configuración de las simulaciones realizadas en este capítulo.

Parámetro	Valor
Tipo escenario	Manhattan 4x4, 6x6 y 8x8 edificios
Dimensiones	900x900, 1350x1350 y 1800x1800 m^2
Modelo movilidad	*Random Walk Obstacle* [31]
Número nodos	114, 238 y 406
Densidad nodos[31]	1 nodo cada 80m
Interfaz radio transmisiones ad-hoc	802.11a en banda de 5.8GHz
Potencia transmisión	17 / 20 dBm
Modelo propagación canal radio	2 Rayos LOS-NLOS Realista
Modelado capa MAC	CSMA/CA, DCF y RTS/CTS.
Modelado efectos de capa física	LUT de *Packet Error Rate* (PER)[32]
Modelo tráfico	Tráfico web [29]
Porcentaje nodos con sesiones activas	15%
Porcentaje nodos egoístas	0/10/20/30/40%

Tabla 5-4 Configuración de parámetros de simulación.

5.5.3 Número de saltos por transmisión multi-salto

Uno de los factores más importantes que influyen en la conectividad de la red es el número de saltos por transmisión multi-salto. En este apartado se evalúan los parámetros y factores que afectan al número de saltos. De acuerdo a la Figura 5-3 anterior, el número de saltos se ve influenciado por tres parámetros: la potencia de transmisión, las dimensiones del escenario y el grado de precisión del modelo de propagación radio utilizado en la simulación. A su vez, estos parámetros influyen también en los factores de la distancia de salto y la distancia total. La distancia total extremo a extremo hace referencia a la suma de las distancias recorridas en cada salto entre el origen y el destino por los paquetes que son recibidos correctamente en el destino. Para ilustrar el significado

[31] Al considerar un escenario Manhattan compuesta por calles y edificios, en la que los nodos se desplazan únicamente por las calles, la densidad de nodos es lineal y se calcula como el cociente entre la suma de la longitud de todas las calles y el número de nodos.

[32] Consultar la sección 4.2.2.

de la distancia total, la Figura 5-5 muestra un ejemplo de transmisión empleando modelos de propagación radio con diferente nivel de precisión. Se considera el modelo de propagación de 2 Rayos para el nodo *1* y el modelo LOS-NLOS para el nodo *3*. Tanto el nodo *1* como el nodo *3* se encuentran a la misma distancia física del punto de acceso, distancia que por lo general no se corresponde con el parámetro de distancia total extremo a extremo. Las diferencias entre ambos modelos es que en el de 2 Rayos el rango de transmisión es mayor que en de LOS-NLOS, y además no se ve afectado por los obstáculos. Por esta razón, el nodo *3* debe establecer una conexión multi-salto a través del nodo *2* y sorteando los edificios, mientras que el nodo *1* puede realizar la conexión con el punto de acceso directamente. Esto hace que la distancia total extremo a extremo sea mayor al considerar el modelo LOS-NLOS. En el modelo de 2 Rayos la distancia sería d_{2R}, mientras que en el modelo LOS-NLOS sería la suma de las distancias d_{LNH} y d_{LNV}.

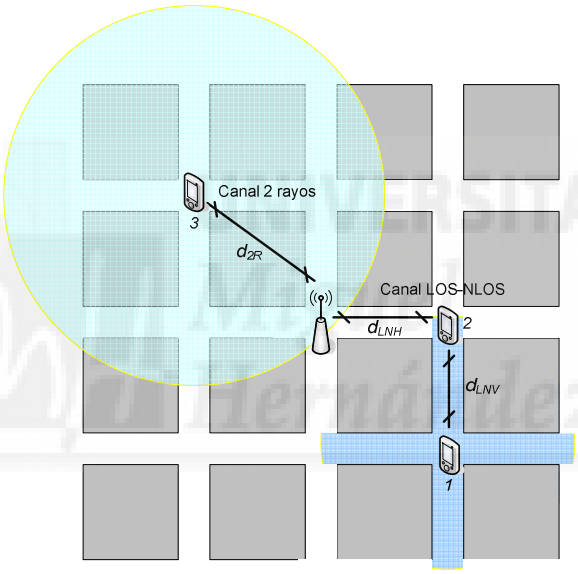


Figura 5-5. Transmisión mediante modelo de propagación de 2 Rayos y LOS-NLOS.

En la Tabla 5-5, que representa la distancia total extremo a extremo, se muestra el efecto de considerar modelos realistas de propagación frente al modelo comúnmente utilizado de 2 Rayos. Se considera como referencia un escenario de tamaño 1350x1350m^2 y potencia de transmisión de 17dBm, en el que no se aplicará ningún tipo de técnica de reputación (el efecto de estas técnicas será analizado más tarde). La Tabla 5-5 muestra un incremento de un 25% en la distancia total recorrida por los paquetes recibidos correctamente, sin nodos egoístas, empleando el modelo LOS-NLOS o el modelo Realista respecto a 2 Rayos. La razón de este incremento se ilustra en la Figura 5-5 anterior, en la que puede observarse que generalmente al usar modelos realistas que consideren la influencia de los obstáculos entre emisor y receptor, la distancia total se ve incrementada debido a que las rutas multi-salto deben sortear los edificios. También se muestra que

aumentar el porcentaje de nodos egoístas (20% y 40%) disminuye la distancia total extremo a extremo. Según la Figura 5-4 anterior, aumenta la probabilidad de que aparezca un nodo egoísta en la ruta, tanto más en las rutas más largas (en los modelos de propagación realistas). Los paquetes perdidos en rutas largas no contribuyen al parámetro de distancia total. Por esta razón, la distancia total se ve reducida al aumentar el porcentaje de nodos egoístas, especialmente en los modelos de propagación LOS-NLOS y Realista. Por otro lado, el tamaño del escenario influye directamente sobre la distancia total, como confirman los resultados mostrados en la Tabla 5-5. La distancia desciende un 31% si se reduce el lado a 900m, mientras que aumenta un 29% en el escenario de 1800m. Estos resultados permiten justificar posteriormente el descenso de la conectividad en el escenario de mayores dimensiones con alta densidad de nodos egoístas.

Lado [m]	Modelo canal	% nodos egoístas		
		0	20	40
1350	2 Rayos	555.21m	526.27m	489.95m
	LOS-NLOS	689.64m (+24.21%)[a]	559.01m (+6.2%)[a]	446.53m (-8.86%)[a]
	Realista	705.41m (+27.05%)[a]	600.57m (+14.1%)[a]	470.94m (-3.88%)[a]
900	Realista	482.57m (-31.59%)[b]	420.74m (-30.0%)[b]	369.85m (-21.47 %)[b]
1800	Realista	913.63m (+29.52%)[b]	706.78m (+17.68%)[b]	512.32 m (+8.79%)[b]

[a] Porcentaje de incremento respecto al modelo de 2 Rayos.
[b] Porcentaje de incremento respecto al escenario con 0% nodos egoístas.

Tabla 5-5 Distancia total extremo a extremo [m].

La Tabla 5-6 confirma lo que intuitivamente cabe esperar: los modelos de canal más precisos también reducen la distancia de salto (distancia entre dos nodos adyacentes en una ruta multi-salto). El valor medio de la distancia de salto para los paquetes recibidos correctamente, se reduce en un 44%, así como también la distancia de salto correspondiente al percentil 95, en un 35% y 25% para LOS-NLOS y Realista, tomando como referencia el modelo de 2 Rayos. Esto se explica porque, para un mismo nivel de potencia de transmisión, los modelos de propagación realistas predicen un descenso mayor de la potencia con la distancia. Por ello, el nivel de potencia de recepción mínimo necesario para la recepción correcta del mensaje se alcanzará a una distancia menor. Por otro lado, un incremento de 3dB en la potencia aumenta la distancia de salto en un 33% para el modelo de 2 Rayos mientras que en el resto el aumento es más moderado (en

torno a un 14%). Un incremento similar se puede apreciar en la Tabla 5-6 para el percentil 95.

Distancia salto [m]	Potencia [dBm]	Modelo canal		
		2 Rayos	LOS-NLOS	Realista
Promedio	17	301.38	166.75 (-44-67%)[a]	171.89 (-42.97%)[a]
	20	400.90 (+33,02%)[b]	189.89 (+13.88%)[b]	198.12 (+15.26%)[b]
Percentil 95	17	403.70	260.87 (-35.38%)[a]	300.27 (-25.62%)[a]
	20	546.46 (+35.36%)[b]	295.11 (+13.13%)[b]	352.09 (+17.36%)[b]

[a] Porcentaje de incremento respecto al modelo de 2 Rayos.
[b] Porcentaje de incremento respecto al escenario con 0% nodos egoístas.

Tabla 5-6 Distancia de salto [m].

La combinación de una distancia total mayor a recorrer por los paquetes y una distancia de salto menor en los modelos realistas al considerar modelos de propación radio realistas, da como resultado un aumento considerable en el número de saltos promedio de las rutas establecidas y el número de saltos promedio por paquete recibido correctamente. En el caso de no aplicar ninguna técnica de reputación y sin nodos egoístas, el aumento en el número de saltos por ruta establecida es de 2.27 (2 Rayos) a 4.97 (LOS-NLOS) y 4.81 (Realista), como se muestra en la Tabla 5-7. El aumento relativo es similar para las técnicas de Marti y PD (la técnica idealista en la que la identidad de los nodos egoístas era conocida de antemano). Otro efecto derivado del incremento del porcentaje de nodos egoístas, desde 0% hasta 40%, es el descenso en el número de saltos promedio de los paquetes recibidos correctamente. Esto se debe a que en las rutas con mayor número de saltos hay más probabilidad de encontrar un nodo egoísta (ver Figura 5-4), y por tanto la ruta o bien será descartada en caso de que se aplique alguna técnica de reputación, o bien los paquetes serán descartados por el nodo egoísta y no contabilizados. En el modelo 2 Rayos este descenso no es relativamente muy notable, de 2.05 saltos a 1.80, lo que supone un -12.2%, mientras que en el modelo Realista esta caída es mucho más acusada, de 4.61 a 2.75 saltos, un -40.35%. Esto se debe a que el número de saltos por ruta establecida es ya de por sí reducido cuando se usa el modelo de 2 Rayos, por las razones ya comentadas (predicción de un menor decrecimiento de la potencia con la distancia y establecimiento de enlaces sin considerar la obstaculización de los edificios como muestra la Figura 5-5).

Técnica	Modelo canal	Número de saltos por ruta establecida	Número de saltos por paquete		
			0%	20%	40%
Sin técnica	2 Rayos	2.27	2.05	1.93 (-5.85%)[b]	1.80 (-12.20%)[b]
	LOS-NLOS	4.97 (+118.94%)	4.47 (+118.05%)[a]	3.43 (-23.27%)[b]	2.64 (-40.94%)[b]
	Realista	4.81 (+111.89%)	4.61 (+124.88%)[a]	3.62 (-21.46%)[b]	2.75 (-40.35%)[b]
Marti	2 Rayos	2.33	2.03	1.99 (-1.97%)[b]	1.99 (-1.97%)[b]
	LOS-NLOS	4.98 (+113.84%)	4.48 (+120.69%)[a]	4.06 (-9.38%)[b]	3.60 (-19.64%)[b]
	Realista	5.06 (+117.09%)	4.61 (+127.09%)[a]	4.22 (-8.46%)[b]	3.89 (-15.62%)[b]
PD	2 Rayos	2.27	2.03	1.98 (-2.46%)[b]	1.94 (-4.43%)[b]
	LOS-NLOS	4.96 (+118.56%)	4.47 (+120.20%)[a]	4.38 (-2.01)[b]	3.87 (-13.42%)[b]
	Realista	4.81 (+112.01%)	4.61 (+127.09%)[a]	4.62 (+0.22)[b]	4.26 (-7.59%)[b]

[a] Porcentaje de incremento respecto al modelo de 2 Rayos.
[b] Porcentaje de incremento respecto al escenario con 0% nodos egoístas.

Tabla 5-7 Número de saltos promedio por ruta establecida y por paquete recibido.

5.5.4 Capacidad de detección de nodos egoístas

Para analizar la influencia de los distintos parámetros reflejados en la Figura 5-3 sobre la capacidad de detección de las técnicas estudiadas, se han propuesto diferentes escenarios, mostrados en la Tabla 5-8. Para cada uno de ellos se muestran los valores promedio de los parámetros de detección discutidos en la sección 5.5.2: el índice de sensibilidad positivo S^+, el índice de error positivo E^+, y el porcentaje de acusaciones falsas. El primer escenario corresponde al tamaño medio con 238 nodos, 17dBm de potencia de transmisión, con sesiones no simultáneas y el modelo de canal radio de 2 Rayos. Para apreciar la influencia del modelado preciso de los efectos del canal radio, en el segundo escenario se emplea el modelo de canal Realista, manteniendo invariantes el resto de parámetros. El tercer escenario es idéntico pero incorpora sesiones simultáneas de tráfico de los usuarios para estudiar el rendimiento de las técnicas de reputación en condiciones de congestión de canal. El cuarto escenario es similar al tercero pero reduce

el tamaño del escenario y el número de nodos a 114. El quinto estudia la influencia de aumentar la potencia de transmisión de 17dBm a 20dBm, manteniendo los mismos valores para el resto de parámetros que el escenario tercero.

Técnica	Parámetro	Escenario				
		I	II	III	IV	V
		Referencia	Modelo de canal	Carga tráfico	Tamaño escenario	Potencia transmisión
Marti	S^+ [%]	98.59	93.87	89.76	90.55	91.14
	E^+ [%]	4.85	10.79	10.80	9.31	10.10
	Acus. Incorrectas [%]	21.93	20.63	36.57	41.36	34.81
TEAM	S^+ [%]	99.98	99.30	98.70	98.86	98.97
	E^+ [%]	41.79	65.52	65.86	59.52	64.24
	Acus. Incorrectas [%]	17.50	30.23	45.18	38.41	43.33

Tabla 5-8 Parámetros de detección de Marti y TEAM en distintos escenarios.

Tanto la técnica de Marti como TEAM obtienen un buen rendimiento en el escenario más simple y con una menor precisión del modelo de canal, con un S^+ próximo a 100%. Además, TEAM mantiene una gran capacidad de detección en todos los escenarios, lo que significa que casi todas las acciones egoístas de los nodos son observadas. Por el contrario, en el caso de la técnica de Marti, el índice S^+ desciende un 4% cuando se consideran efectos del canal radio realistas en el segundo escenario, y alrededor de un 9% en el canal con congestión en el escenario tercero. La degradación de la capacidad de detección de la técnica *watchdog* al considerar estos factores se debe al aumento de las caídas del enlace radio, tal y como se explicó en el apartado 5.2. Al aumentar las caídas de enlace radio, hay un mayor porcentaje de ocasiones en que el *watchdog* no puede distinguir si realmente el nodo retransmisor ha descartado el paquete, y esto provoca el descenso del número de acciones egoístas observadas correctamente y de S^+. El valor del parámetro S^+ no cambia cuando se varían las dimensiones del área de simulación o la potencia de transmisión, en los escenarios cuarto y quinto respectivamente. Por lo tanto puede concluirse que sólo la precisión del modelo de propagación radio y las colisiones provocadas por la carga de tráfico influyen en la capacidad de detección de las técnicas de reputación.

Por otro lado, el modelado preciso de los efectos de canal en el segundo escenario incrementa el número de veces en que acciones cooperativas se confunden con acciones egoístas, incrementando el índice de error positivo E^+. Esto se debe a la dificultad del mecanismo de observación *watchdog* para distinguir las acciones cooperativas, en

presencia de errores de transmisión radio y colisiones de paquetes, como se comentó en el apartado 5.2. Tal y como se mostró en el apartado 5.5.3, el número de saltos de las transmisiones multi-salto se incrementa al aumentar la precisión del modelado de los efectos del canal en los escenarios segundo al quinto. Es especialmente apreciable comparando los escenario primero y segundo, que son idénticos salvo en este aspecto. Debido al incremento en el número de saltos y a la dificultad del mecanismo *watchdog* de observar correctamente los comportamientos egoístas cuando los efectos del canal se modelan de manera precisa, la red está más expuesta a los nodos egoístas y su capacidad para combatirlos disminuye. El incremento en el número de observaciones de descarte incorrectas aumenta el porcentaje de acusaciones falsas en los escenarios en los que se modela la propagación en el canal de manera precisa. Sin embargo, debe subrayarse que ambas figuras no son completamente equivalentes: el porcentaje de acusaciones falsas se refiere al cociente entre las acusaciones falsas y las acusaciones totales, mientras que E^+ se refiere al cociente entre el número de observaciones de descarte incorrectas y el número de veces que se requiere que un nodo cooperativo retransmita un paquete. Las acciones egoístas de un nodo pueden ser detectadas por muchos otros nodos, pero puede que sólo sea acusado por una parte de ellos, cuando las condiciones de acusación en la técnica de reputación ejecutada en alguno de ellos se cumplan. También es reseñable que incluso un índice de error no muy alto del *watchdog* en torno al 10% en Marti, se traduce en un porcentaje de acusaciones incorrectas de un 35% en los escenarios con congestión de canal (del tercero al quinto). El incremento en las acusaciones incorrectas dificulta la tarea de encontrar rutas seguras, es decir, sin nodos egoístas conocidos, dado que habrá más nodos a evitar durante los procesos de establecimiento de ruta.

Tal y como muestra la Tabla 5-8, aparentemente TEAM aumenta el índice de error positivo E^+ respecto a la técnica Marti. La razón es que mientras que para elaborar esta métrica para Marti sólo se han considerado las observaciones directas, en la técnica TEAM se tomaron tanto las observaciones directas como las indirectas, dado que TEAM contabiliza ambos tipos de reputación. Recuérdese del apartado 5.2 que en la reputación directa es el nodo precursor el que observa la retransmisión, mientras que en la reputación indirecta es un nodo vecino el que observa tanto la transmisión del nodo precursor al retransmisor, como la retransmisión de este último. Como se explicó, y puede comprobarse en los resultados de la Tabla 5-8, las observaciones indirectas están sujetas a un mayor error, dado que no siempre el nodo retransmisor está en el rango de transmisión del nodo observador (lo cual generalmente sí se cumple en el caso de las observaciones directas) y de ahí que haya un considerable aumento del número de errores, especialmente cuando se consideran condiciones de LOS-NLOS en los modelos de canal más precisos en el escenario, como es el caso en el segundo y posteriores. Sin embargo, la imprecisión de la reputación indirecta tiene un impacto moderado sobre el porcentaje de

acusaciones incorrectas, debido a que la reputación indirecta está ponderada por un coeficiente mucho menor que la reputación directa en el cálculo de la confianza de nodo de la técnica TEAM. En definitiva, los resultados obtenidos muestran claramente el notable impacto que las condiciones de propagación radio y el modelado del tráfico pueden tener sobre el funcionamiento de las técnicas de reputación, y en particular sobre su capacidad de detectar de manera precisa a los nodos egoístas.

5.5.5 Tasa de entrega y pérdidas de paquetes

Finalmente se presentan una serie de diagramas de barras en las Figuras 5-6 a 5-9 que muestran el rendimiento promedio de la red en distintos escenarios. Cada barra apilada corresponde a un parámetro: la tasa de entrega de paquetes o PDR (*Packet Delivery Ratio*), porcentaje de paquetes perdidos por la no disponibilidad de rutas (etiqueta "sin ruta") o por caídas de enlaces (etiqueta "caída de enlace"), porcentaje de paquetes descartados por nodos egoístas (etiqueta "egoísta"), y porcentaje de paquetes descartados por proceder de una ruta con nodos egoístas (etiqueta "no seguro"). Cada grupo de cinco barras representa una técnica de reputación diferente en las Figuras 5-6 a 5-8: "sin TR" (sin Técnica de Reputación), Marti, TEAM y PD. Cada barra corresponde a un porcentaje de nodos egoístas, creciente de 0% a 40%. Las Figuras 5-6 y 5-7 corresponden a los modelos de 2 Rayos, y Realista respectivamente, con sesiones no simultáneas, mientras que en la 5-8 se emplea el modelo Realista y sesiones simultáneas. Se ha considerado el escenario de 238 nodos con potencia de transmisión de 17dBm en las Figuras 5-6 a 5-8. Comparando la Figura 5-6 y la 5-7 se puede apreciar el efecto de emplear un modelo de propagación que tiene en cuenta efectos realistas. Se aprecia un descenso notable del PDR debido sobre todo a un porcentaje mayor de paquetes descartados por los nodos egoístas, salvo en la técnica PD, donde los paquetes no son enrutados por el resto de nodos dado que proceden de nodos egoístas. Las técnicas de Marti y TEAM disminuyen el porcentaje de paquetes descartados por los nodos egoístas, respecto a no utilizar técnica de reputación. Sin embargo, el nivel de paquetes descartados por nodos egoístas usando estas técnicas es alto. Esto se debe a que la detección de los nodos es local, y en las técnicas empleadas no se establece un procedimiento para propagar la identidad de los nodos egoístas entre los nodos. Así, aunque un nodo egoísta sea detectado por un nodo, su aislamiento será difícil si los demás nodos no conocen también su identidad. Este problema se abordará en el capítulo 8. Por otro lado, con la técnica PD ningún nodo egoísta tiene ocasión de descartar paquetes, porque su identidad es conocida por todos los nodos. En este caso, la mayoría de descartes se debe a la no disponibilidad de rutas, debido a que los nodos egoístas no pueden hallar ninguna ruta. El descenso del PDR en la Figura 5-7 respecto a la Figura 5-6 está justificado por los tres factores mostrados anteriormente: primero, el empleo de un modelo realista disminuye el PDR *per se*;

además, el incremento del número de saltos promedio de las transmisiones disminuye las probabilidades de encontrar una ruta libre de egoístas; por último, la capacidad de detección de nodos egoístas de la técnica *watchdog* también es menor.

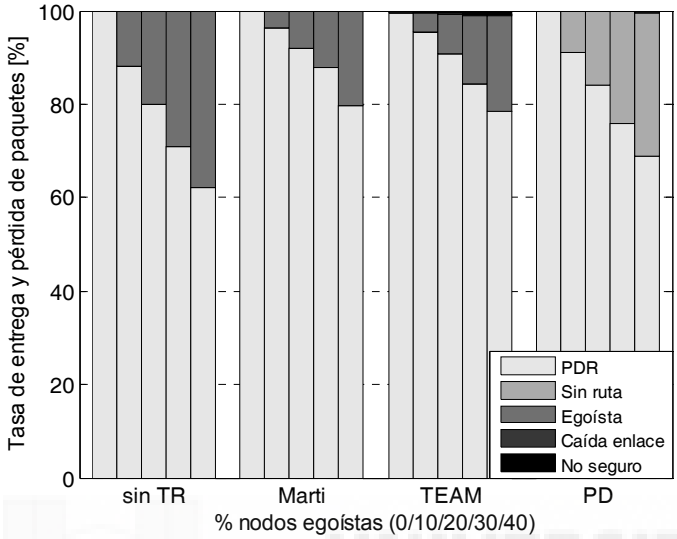


Figura 5-6. PDR de distintos protocolos considerando el modelo de propagación de 2 Rayos.

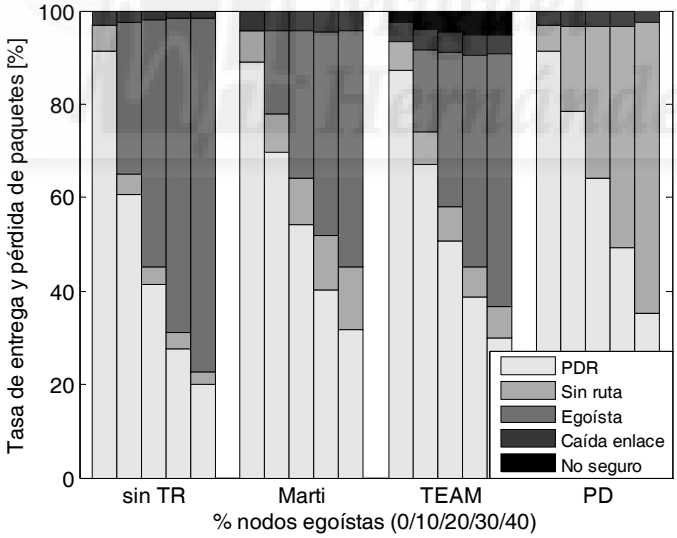


Figura 5-7. PDR de distintos protocolos considerando el modelo de propagación Realista.

En el escenario con carga alta de la Figura 5-8, se observa que el descenso en PDR está causado también por un aumento en el número de paquetes sin ruta, debido a la congestión en la red, y en menor medida, también por la peor capacidad de detección de *watchdog* en estas condiciones, que incrementa las acusaciones incorrectas, como reflejaba la Tabla 5-6. Este problema será abordado en el capítulo 6.

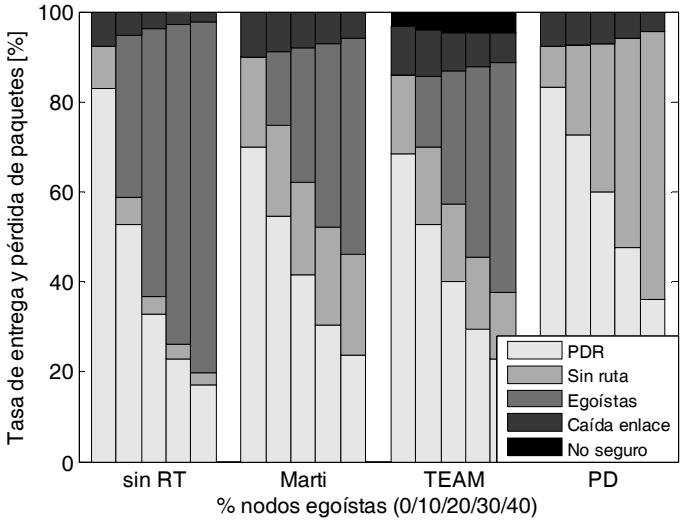


Figura 5-8. PDR de distintos protocolos considerando el modelo de propagación Realista y una carga de tráfico elevada.

Finalmente, la Figura 5-9 refleja la influencia de los factores que modifican el número de saltos, considerando para todos los casos la técnica TEAM. El primer grupo de columnas corresponde al escenario de referencia de 238 nodos y potencia 17dBm, mientras que en el segundo se aumenta la potencia a 20dBm, en el tercero se disminuye el tamaño del escenario (114 nodos) y en el último se aumenta (406 nodos). Los resultados confirman que el porcentaje de paquetes descartados disminuye siempre que en el escenario hay un promedio de saltos menor, como al aumentar la potencia o disminuir el tamaño, mientras que aumenta considerablemente al aumentar el tamaño del escenario.

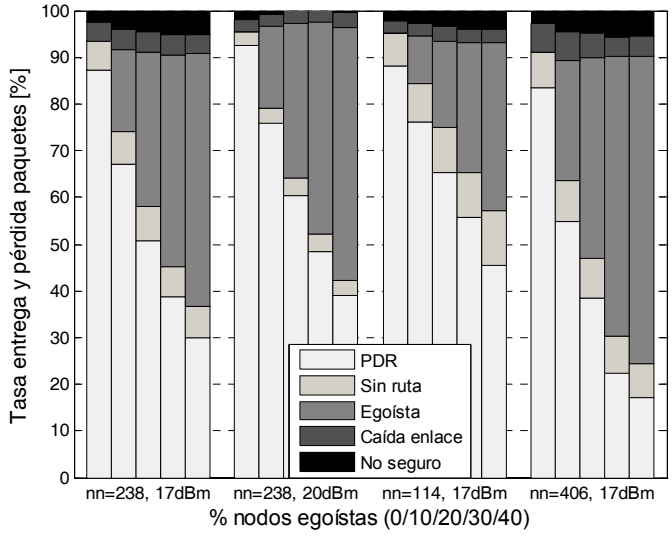


Figura 5-9. PDR de la técnica TEAM considerando el modelo de propagación Realista y distintas condiciones del escenario.

5.6 Conclusiones

En redes MANET la conectividad y funcionalidad de la red puede verse amenazada por aquellos nodos que se niegan a retransmitir paquetes para los demás. Dado que las funciones de red se realizan de manera descentralizada en este tipo de redes, deben proponerse técnicas para incentivar a los nodos a cooperar en el mantenimiento de la red y en la retransmisión de los paquetes de datos y de señalización.

En la literatura se han propuesto técnicas de incentivo a la cooperación de distintos tipos. Las características más destacables de las basadas en reputación son su escalabilidad, su naturaleza completamente distribuida y su implementación directa. Las técnicas de cooperación basadas en reputación se basan en la observación del comportamiento del resto de los nodos, y en la elaboración de tablas de reputación que se emplean para guiar los procesos de enrutamiento, en los que se evitará utilizar rutas en las que participen nodos egoístas. También, y como represalia contra aquellos nodos que exhiban un comportamiento egoísta y que hayan sido detectados, se evitará retransmitir paquetes con origen o destino en nodos egoístas conocidos. El rendimiento de estas técnicas depende de la precisión y la rapidez con que sean capaces de determinar qué nodos se comportan egoístamente. Para ello además se necesita una técnica que permita observar el comportamiento de los nodos. La técnica más extendida es la de *watchdog*, empleada por primera vez en el protocolo de Marti. Esta técnica se basa en escuchar de manera promiscua las transmisiones que se realizan en el rango de comunicaciones del nodo, para detectar que el nodo siguiente en la comunicación multi-salto realiza correctamente la retransmisión. *Watchdog* es la técnica de observación más extendida y aceptada en la literatura, pero el rendimiento de las técnicas que lo utilizan no ha sido evaluado en condiciones realistas, por lo que las conclusiones extraídas deben ser comprobadas en un entorno de simulación más preciso. En concreto, el objetivo del capítulo era determinar hasta que punto unas condiciones realistas de simulación, con diferentes grados de congestión del canal y con modelos de propagación radio más precisos, influían en el rendimiento de estas técnicas. Para ello se ha evaluado el rendimiento de dos técnicas de reputación: la de Marti, como referencia dado que fue el primero en proponer y utilizar el *watchdog*, y la técnica TEAM, más avanzada y reciente y que incorpora algunas características mejoradas respecto al protocolo de Marti.

En los resultados obtenidos se ha analizado la influencia de ciertos parámetros de simulación y dimensionado sobre la eficiencia de estas dos técnicas. Los factores claves de su rendimiento en presencia de nodos egoístas son la capacidad de detección de la técnica *watchdog* y el número de saltos promedio de las transmisiones multi-salto. Estos elementos no habían sido estudiados suficientemente hasta ahora, dado que no se habían considerado importantes parámetros de simulación con una notable influencia en estos

factores. Los resultados obtenidos han demostrado la conveniencia de emplear un modelo de canal realista para un correcto estudio de los factores mencionados, así como la necesidad de incentivar a los nodos egoístas a cambiar su estrategia, puesto que un porcentaje elevado de los mismos afecta muy negativamente al rendimiento final de la red, independientemente de la capacidad de detección del sistema de prevención que se aplique. También se ha observado que el rendimiento de ambas técnicas de reputación se deteriora notablemente al ser evaluado en condiciones realistas de simulación. En este punto, se hace necesario proponer técnicas que contrarresten este deterioro, y en especial, que ataquen el problema de las acusaciones incorrectas, que provocan un deterioro notable de la conectividad de la red. Este será el tema del siguiente capítulo.

UNIVERSITAS
Miguel
Hernández

6

Nuevas propuestas de técnicas de reputación distribuidas

En el capítulo anterior se evaluaron las técnicas de reputación Marti y TEAM, y se comprobó que al ser evaluadas en diferentes condiciones de simulación que trataban de aproximarse a condiciones realistas, su rendimiento se deterioraba apreciablemente. Este deterioro era similar en ambas técnicas, y proviene en realidad del error en el proceso de observación de la retransmisión de los paquetes al que está sujeta la técnica *watchdog*. *Watchdog* es una técnica que permite comprobar la correcta retransmisión de los paquetes por parte de los nodos vecinos, a través de la escucha de las retransmisiones con la MAC del nodo observador en modo promiscuo (es decir, escuchando todos los paquetes, incluidos aquellos no específicamente dirigidos al nodo). De esta manera, si el paquete es retransmitido por el nodo retransmisor, el nodo observador lo escucha también y registra una acción cooperativa del nodo. Pasado un cierto límite de tiempo, si el nodo observador no escucha la retransmisión, se para el temporizador y se registra una acción negativa. Sin embargo, errores de propagación radio y colisiones de paquetes pueden impedir que el nodo observador escuche correctamente la retransmisión. Este efecto se ha hecho evidente al analizar las técnicas en condiciones realistas, es decir, considerando modelos de propagación realistas (que incluyen efectos como el desvanecimiento rápido y lento o condiciones de visibilidad) y con una carga de tráfico moderada.

Las técnicas de reputación como Marti y TEAM registran y procesan la información proveniente de la técnica *watchdog* para decidir aquellas rutas que son más convenientes para enrutar los propios paquetes, evitando aquellas rutas con nodos egoístas, y al mismo tiempo evitando establecer rutas para retransmitir los paquetes procedentes de nodos egoístas como medida de castigo. Debido al error en las observaciones de *watchdog*, algunos nodos cooperativos son acusados erróneamente y potenciales rutas seguras son descartadas. Esto limita la capacidad de los nodos de encontrar rutas seguras para enrutar los propios paquetes, ya sea porque sean acusados injustamente o porque acusen injustamente a otros nodos. En definitiva, se hace necesario encontrar estrategias que compensen la inexactitud de *watchdog* y rebajen el nivel de acusaciones incorrectas para mejorar la conectividad de las redes MANET. Este es el propósito del presente capítulo. En primer lugar se presentan las tres estrategias propuestas para la compensación del error introducido por *watchdog*. Para cada una de ellas, se expone el objetivo perseguido, su funcionamiento y también los potenciales inconvenientes. Posteriormente se detallan los procedimientos experimentales llevados a cabo para comprobar el funcionamiento de las estrategias propuestas de manera comparativa, tomando como referencia de base las técnicas Marti y TEAM.

6.1 Reset Activity Mode

La primera propuesta, denominada *Reset Activity Mode* (RAM), tiene como objetivo reducir el número de acusaciones incorrectas debidas a la alta variabilidad del canal radio o a las colisiones de paquetes. La situación que RAM trata concretamente de mejorar es la excesiva penalización por el registro de acciones egoístas, teniendo en cuenta el número de ocasiones en que *watchdog* realiza observaciones incorrectas. Para evitar que dichas observaciones provoquen finalmente una acusación incorrecta por parte de las técnicas de reputación, tales como la de Marti y TEAM que se han implementado en este trabajo, RAM incrementa los efectos sobre la reputación de las acciones cooperativas observadas. En la implementación original de estos protocolos, los nodos acumulan buena o mala reputación en función del comportamiento observado por el resto de los nodos. Si se detecta que un nodo está descartando paquetes repetidamente, será acusado de actuar egoístamente y será aislado. Sin embargo, tal y como se demostró en el quinto capítulo, esto puede provocar acusaciones incorrectas si algún nodo no es capaz de escuchar correctamente la retransmisión de los paquetes. Esto puede deberse a colisiones de paquetes provocadas por la congestión en el canal, y a errores de transmisión, los cuales se interpretan como descartes intencionados de paquetes. Para evitar estas acusaciones incorrectas, RAM incrementa la contribución de las retransmisiones observadas a la reputación del nodo. Para ello, define algunas acciones que el nodo observador debe

realizar tras observar la retransmisión de un paquete. Concretamente, cuando *watchdog* detecta la retransmisión de un paquete, se restaura la reputación del nodo retransmisor en la tabla de reputación al nivel de un nodo con categoría "desconocido", en caso de que hubiera sido degradado por debajo de ese nivel. Además, si la técnica de reputación considerada lleva la cuenta de faltas que el nodo retransmisor acumula, la cuenta se iguala a 0. Además, el nodo observador descarta los paquetes que mantiene en el buffer del *watchdog* a la espera de que se escuche su retransmisión, y por tanto no se computa ninguna falta por estos paquetes. Es importante señalar que RAM no se aplica a nodos que ya hayan sido acusados de actuar egoístamente, sino solo a los nodos con categoría "cooperativo". Los nodos egoístas no podrán recuperar su reputación hasta que finalice el *Tiempo de Aislamiento*. El pseudocódigo de la propuesta se muestra en la Figura 6-1.

Técnica RAM
Evento detección de retransmisión Categoría nodo retransmisor "cooperativo"? → SÍ: Reputación nodo menor que "desconocido"? → SÍ: Restaurar reputación nodo Resetear número faltas nodo retransmisor Descartar paquetes pendientes de escucha retransmisión

Figura 6-1. Pseudocódigo de la técnica RAM.

Cabe señalar cierta circunstancia en la que sería desaconsejable aplicar la técnica RAM. Hasta este capítulo, el modelo de nodo egoísta considerado descartaba todos los paquetes que debía retransmitir, tal y como se explicó en el apartado 5.1. Sin embargo, podría identificarse otro tipo de nodo egoísta que descartara de manera aleatoria no todos los paquetes sino únicamente una cierta proporción de ellos. En este caso, dependiendo de la proporción de paquetes que sean descartados, podría ocurrir que RAM contribuyera a restaurar de manera incorrecta la reputación de nodos realmente egoístas, facilitando que no sean detectados y por tanto incrementando el número de paquetes descartados por egoístas y el número de rutas establecidas con nodos egoístas. Sin embargo, debe señalarse que este efecto indeseado sólo sería posible cuando la proporción de paquetes descartados por los egoístas fuera muy baja. Si la proporción de paquetes descartados es alta, entonces RAM sigue siendo efectivo, ya que es más probable que el nodo sea detectado antes de que una eventual retransmisión por parte del nodo haga que RAM restaure su reputación. De esta manera, el perjuicio causado por estos nodos está limitado, ya que o bien son nodos que aunque no son detectados descartan pocos paquetes, o bien son nodos más egoístas pero que sí son detectados incluso considerando RAM. Aún así,

en el capítulo 7 se proponen y evalúan estrategias más sofisticadas capaces de detectar más fiablemente este tipo de comportamientos.

6.2 Warning Mode

La propuesta WM (*Warning Mode*) está también diseñada para impedir acusaciones incorrectas provocadas por errores de transmisión radio y colisiones de paquetes, pero con una metodología diferente. En la implementación original de las técnicas basadas en reputación consideradas en este trabajo, cuando el nodo retransmisor exhibía un comportamiento negativo durante un cierto tiempo, es directamente marcado como egoísta, y los enlaces en los que participa el nodo se rompen. Por el contrario, WM introduce una categoría intermedia, la categoría "sospechoso", situada entre un nodo "neutral" y un nodo marcado como "egoísta". La categoría "sospechoso" funciona como una advertencia a los nodos de los cuales se sospecha que tienen un comportamiento egoísta. Antes de que sean marcados definitivamente como egoístas, reciben otra oportunidad para recuperarse de la mala reputación.

El mecanismo con el que funciona WM es el siguiente. Cuando las condiciones para acusar a un nodo se cumplen, se le marca primero como sospechoso, y el enlace establecido con el nodo se rompe temporalmente. Estas condiciones varían según la técnica de reputación considerada. En la técnica de Marti, un nodo es acusado de actuar egoístamente cuando el número de faltas contabilizadas supera el *Límite Máximo de Faltas*. Por otro lado, en TEAM, un nodo retransmisor es acusado cuando su reputación es menor que el *Límite de Reputación*. Los nodos con categoría "sospechoso" pueden participar en las tareas de enrutamiento y encaminamiento de paquetes, pero se aplican algunas restricciones adicionales para mitigar el posible incremento en el número de paquetes descartados por los nodos realmente egoístas. En particular, los nodos actuaran con los nodos "sospechosos" como si fueran nodos "neutrales", pero los mecanismos que controlan la observación y la acusación de los nodos se reajustan para reducir el número de paquetes de datos adicionales descartados por nodos potencialmente egoístas. En primer lugar, el *Tiempo Límite* del que dispone un nodo para retransmitir un paquete se reduce en un factor α. En este trabajo el *Tiempo Límite* de retransmisión para nodos cooperativos está fijado a 50ms. Para los nodos sospechosos se aplica un factor α=0.5, que da lugar a un *Tiempo Límite* de 25ms, siguiendo el compromiso entre la reducción del tiempo necesario para detectar a los potenciales nodos egoístas y el incremento en el número de paquetes retransmitidos no detectados. En simulaciones preliminares pudo constatarse que con un *Tiempo Límite* de retransmisión de 25ms, únicamente un 2% de paquetes retransmitidos no eran escuchados por el nodo observador. La reducción del *Tiempo Límite* de retransmisión en WM tiene como objetivo reducir el tiempo necesario

para confirmar si un nodo "sospechoso" es realmente egoísta. En este contexto, la observación de un descarte adicional es suficiente para acusar como egoísta a un nodo ya declarado "sospechoso". Para ello, se debe modificar el funcionamiento de la técnica de reputación específica. Cuando se observa un descarte, si el nodo retransmisor había sido marcado previamente como "sospechoso", entonces se debe acusar al nodo siguiendo el procedimiento especificado en la técnica de reputación. Si el nodo retransmisor no es un nodo marcado como "sospechoso", entonces no se necesita ninguna adaptación especial de la técnica de reputación. Por otro lado, si un nodo observa que un nodo catalogado como "sospechoso" vuelve a cooperar otra vez, entonces su reputación se reseteará al nivel asignado por defecto a nodos marcados como "desconocido", con el fin de darle la oportunidad de recuperarse de la mala reputación acumulada, que podría haber sido provocada por colisiones de paquetes o errores de transmisión radio. Las acciones específicas que las técnicas de reputación deben realizar dependen del funcionamiento específico de cada una. En la técnica de Marti, se resetean el contador de faltas y el nivel de reputación del nodo retransmisor. En el caso de la técnica TEAM, se consideran los dos tipos de reputaciones que dependen de *watchdog*: reputación directa e indirecta, y se restauran al valor *Límite de Reputación* asignado a los nodos marcados como "desconocidos".

El beneficio esperado con la aplicación de WM viene del hecho de que, en la implementación original del *watchdog*, errores de transmisión radio esporádicos, desvanecimientos y colisiones de paquetes pueden provocar un incremento perjudicial del número de acusaciones incorrectas. Al contrario, usando el modo WM, los nodos "sospechosos" tienen una oportunidad extra para recuperarse de una mala reputación asignada injustamente. En caso de que la mala reputación sea consecuencia de colisiones de paquetes o errores de transmisión radio, el nodo "sospechoso" puede volver a incorporarse a la comunicación durante el proceso de búsqueda de ruta posterior a la rotura del enlace provocado por la técnica de reputación y recuperar su reputación, una vez que las condiciones de transmisión han mejorado. Si las condiciones de transmisión no mejoran, no es probable que el nodo "sospechoso" pueda participar en el proceso de búsqueda de ruta, y por tanto el nodo no sería acusado, lo cual en caso de que no sea egoísta es beneficioso, ya que se evita la acusación de un nodo cooperativo. De esta manera, el nodo observador busca una ruta alternativa, y el nodo retransmisor evita ser acusado de manera injusta. Por otro lado, si el nodo "sospechoso" actúa realmente de manera egoísta, y sí participa en la nueva ruta establecida, entonces será rápidamente detectado tras sólo algunos descartes de paquetes más, debido al endurecimiento de las condiciones de vigilancia establecido por WM para los nodos "sospechosos", y será rápidamente aislado. También cabe la posibilidad de que el nodo retransmisor y el nodo observador que lo marcó como "sospechoso" no vuelvan a interactuar otra vez debido a la

movilidad de los nodos. En ese caso, no se realizará una acusación de nodo egoísta, y aunque esto es posible que disminuya el número de acusaciones correctas realizadas, por otro lado no tiene una repercusión negativa en el número de paquetes descartados por los nodos egoístas, ya que en definitiva el nodo observador no volverá a usar al nodo marcado como "sospechoso" como retransmisor. El pseudocódigo de la propuesta WM se muestra en la Figura 6-2.

Técnica WM
Evento detección de descarte paquete Es un nodo "sospechoso"? → SÍ: Iniciar acusación definitiva nodo NO: Se cumplen condiciones acusación? → SÍ: Marcar nodo como "sospechoso" Romper enlace y buscar ruta Ajustar *Tiempo Límite* retransmisión del nodo NO: Seguir indicaciones protocolo
Evento detección de retransmission Es un nodo "sospechoso"? → SÍ: Restaurar reputación nodo nivel "desconocido" Resetear número faltas NO: Seguir indicaciones protocolo

Figura 6-2. Pseudocódigo de la técnica WM

6.3 Reset Failure Mode

El modo *Reset Failure Mode* (RFM) tiene como objetivo combatir aquellas acusaciones incorrectas provocadas por caídas de enlace entre el nodo observador y el nodo retransmisor, o entre el nodo retransmisor y el nodo sucesor. Las caídas de enlace pueden ser provocadas por efectos del canal como el desvanecimiento o la movilidad de los nodos. La capa MAC dispone de un mecanismo para detectar las caídas de enlace y se encarga de iniciar un evento de caída de enlace para informar al protocolo de enrutamiento. El protocolo de enrutamiento transmite entonces un mensaje de "Error de Ruta" para informar de la caída del enlace a aquellos nodos que estén usándolo. Sin embargo, antes de que se dispare el evento de caída de enlace y se transmita el mensaje de "Error de Ruta", algunos de los paquetes que el nodo observador esperaba escuchar

puede que no hayan sido retransmitidos por el nodo retransmisor. Por consiguiente, las copias de los paquetes en el buffer de paquetes caducarán, y la reputación del nodo retransmisor será disminuida injustamente. Para evitar esta situación en presencia de caídas de enlace, RFM restaura la reputación del nodo retransmisor en la tabla del nodo observador al nivel de reputación asignado por defecto a nodos con categoría "desconocido". El término "desconocido" hace referencia a la categoría por defecto asignada a un nodo que aparece en la tabla de reputación por primera vez. Además, RFM borra del buffer de paquetes del nodo observador aquellos paquetes cuya retransmisión está pendiente de escuchar, independientemente de su *Tiempo Límite de Retransmisión*, ya que el nodo no podrá retransmitirlos.

La implementación del modo RFM depende de la técnica considerada. Cuando se aplica al protocolo de Marti, debe evaluarse el nivel de reputación del nodo retransmisor. Si ha sido previamente rebajado por debajo del nivel correspondiente a la categoría "desconocido", se resetea a ese valor y el número de faltas se iguala a 0, dado que se asume que esas faltas han sido provocadas por la rotura del enlace y no por el comportamiento egoísta del nodo. Si se aplica al protocolo TEAM, el modo RFM sólo modifica la reputación de los nodos, dado que el número de faltas no es un parámetro que se tenga en cuenta. En este caso, el modo RFM incrementa en cierto valor la reputación directa e indirecta del nodo retransmisor de manera proporcional al número de paquetes *np* que estaban pendientes de ser retransmitidos en el buffer del nodo observador en el momento de la caída del enlace. En concreto, los niveles de reputación se ajustan siguiendo la expresión:

$$R_1 = R_0 + k \cdot np \tag{6-1}$$

donde R_0 y R_1 representan los niveles de reputación (directa o indirecta) antes y después del reajuste realizado por el modo RFM tras una rotura de enlace. El parámetro k ha sido ajustado a 0.1, que es el valor de penalización aplicado a la reputación directa o indirecta de un nodo al detectarse una no retransmisión en la implementación original de TEAM. Debe señalarse que las excepciones establecidas en el modo RFM se usan solo cuando el nodo retransmisor es todavía visto por el nodo observador como no egoísta. Si el nodo retransmisor es acusado antes de que el evento de caída de enlace se dispare, entonces no se cambia el procedimiento usual de acusación de la implementación original de la técnica de reputación correspondiente.

Una desventaja potencial de RFM es que en algunos casos, la restauración de la reputación tras roturas de enlace podría incrementar la reputación de nodos realmente egoístas. Esto podría pasar si se detectara una caída del enlace, y el nodo siguiente en la ruta fuera un nodo egoísta que todavía no ha sido descubierto. Sin embargo, es importante

señalar que esto ocurriría únicamente en transmisiones multi-salto en la que los enlaces tuvieran un período de vida muy corto, lo cual en realidad debe ser evitado mediante el empleo de protocolos de enrutamiento *ad-hoc* eficientes. Además, es más probable que el tiempo de vida medio de los enlaces sea mayor que el tiempo necesario para detectar a los nodos egoístas en escenarios con movilidad reducida o moderada, donde son factibles las comunicaciones multi-salto cooperativas. El pseudocódigo de la propuesta RFM se presenta en la Figura 6-3.

Técnica RFM
Evento detección caída enlace Reputación nodo retransmisor menor que "desconocido"? → SÍ: Resetear número faltas nodo retransmisor Borrar paquetes pendientes de escucha retransmisión Restaurar nivel reputación nodo retransmisor

Figura 6-3. Pseudocódigo de la técnica RFM

6.4 Evaluación

6.4.1 Métricas de evaluación

Las técnicas propuestas han sido diseñadas para mejorar la precisión de detección de las técnicas de reputación que usan el mecanismo de detección *watchdog*. Esta mejora incrementará el rendimiento y la conectividad general de la red gracias a la mejor capacidad para identificar de manera rápida y exacta a los nodos cooperativos y egoístas; esta capacidad incrementará a su vez el número de rutas multi-salto seguras disponibles. En este contexto, las técnicas de Marti y TEAM presentadas en el capítulo 5 han sido seleccionadas como referencia con la cual comparar el rendimiento de las mejoras propuestas frente a la implementación original de las técnicas.

Para evaluar el rendimiento de las técnicas, se analizarán primero una serie de parámetros que relacionan las mejoras apreciables en términos de reputación con las mejoras en la conectividad. Estos parámetros de reputación son el número de acusaciones, el número de establecimientos de ruta y el número de negaciones de ruta. El número de acusaciones se refiere al total de acusaciones realizadas durante toda la simulación por parte de algún nodo hacia algún otro nodo. Por acusaciones correctas se entienden aquellas que se dirigen a nodos egoístas, mientras que las acusaciones incorrectas recaen sobre nodos cooperativos y están provocadas por errores en la

observación de *watchdog*. El objetivo de precisión exige minimizar el número de acusaciones incorrectas y maximizar el número de acusaciones correctas, lo cual se traduce en una mayor disponibilidad de rutas sin ningún nodo egoísta y en un número mayor de rutas con nodos egoístas (y por tanto, a evitar) identificadas, lo cual repercute en una mayor conectividad. Para apreciar dicha relación, se estudiarán los parámetros de número de establecimientos de ruta correctos (aquellos en los que la ruta no contiene ningún nodo egoísta) y establecimientos de ruta incorrectos (aquellos en los que la ruta contiene algún nodo egoísta); el objetivo será minimizar los establecimientos de ruta incorrectos y maximizar los correctos. Minimizar el establecimiento de rutas incorrectas disminuirá el número de paquetes descartados por nodos egoístas, mientras que maximizar el establecimiento de rutas correctas disminuirá el número de paquetes para los cuales el protocolo de enrutamiento no encuentra una ruta multi-salto adecuada para la transmisión. Finalmente, y también relacionado con el número de acusaciones, se estudiará el número de negaciones de ruta (aquellas peticiones de búsqueda de ruta que han sido negadas por creer que había algún nodo egoísta en la ruta); pueden ser negaciones de ruta correctas (había algún nodo egoísta en la ruta y por tanto era deseable que no se estableciese) o incorrectas (no había ningún nodo egoísta en la ruta). Al igual que antes, este parámetro se relaciona directamente con la conectividad: a mayor número de negaciones correctas, menor número de paquetes descartados por egoístas, y a mayor número de negaciones incorrectas, mayor número de paquetes descartados sin ruta.

El parámetro más importante para medir la conectividad de manera directa será el PDR (*Packet Delivery Ratio*), el cual hace referencia al porcentaje de paquetes recibidos correctamente frente al total de paquetes transmitidos. Maximizar este parámetro es el objetivo final de las propuestas, para lo cual deben minimizarse aquellas ocasiones en las que los paquetes son descartados y por tanto no son entregados al destino. Para medir esta circunstancia se usan los parámetros siguientes: porcentaje de paquetes descartados sin ruta, porcentaje de paquetes descartados por nodos egoístas, porcentaje de paquetes descartados por caída de enlace, y porcentaje de paquetes descartados por su origen no seguro. Los paquetes descartados sin ruta son aquellos que no han podido retransmitirse porque el protocolo de enrutamiento era incapaz de hallar una ruta válida. Los paquetes descartados por nodos egoístas son aquellos que al alcanzar en la transmisión multi-salto un nodo egoísta en la ruta, son descartados. Los paquetes descartados por caída de enlace son aquellos paquetes que esperaban en el buffer de una ruta a ser transmitidos, y son descartados cuando el enlace se cae. Los paquetes descartados por su origen no seguro son aquellos que son descartados por un nodo al detectar que provienen de algún nodo acusado de actuar egoístamente.

Finalmente, el parámetro de la latencia de la red mide el tiempo medio necesario para la transmisión de los paquetes desde el origen al destino. Se espera que la mayor

disponibilidad de rutas con las técnicas propuestas reduzca la latencia media de los paquetes.

6.4.2 Escenarios de simulación

Para evaluar el rendimiento de las técnicas propuestas se han llevado a cabo simulaciones a nivel de sistema para emular el funcionamiento de una red móvil inalámbrica multi-salto usando la plataforma de simulación ns-2 modificada con las ampliaciones descritas en el capítulo 4 y con la extensión del Rice Monarch Project [24] para redes móviles y multi-salto. Las condiciones de simulación también fueron presentadas de manera general en el capítulo 4. El entorno de simulación corresponde a un escenario tipo Manhattan con edificios distribuidos en una celda de 6x6 edificios cuadrados de 200m de lado con 25 metros de calle entre cada edificio, completando unas dimensiones totales de 1350x1350m^2. En este escenario los transeúntes caminan siguiendo el modelo *Random Walk Obstacle* [31]. La densidad promedio de los nodos es de uno por cada 80m a lo largo de las calles. Este valor permite el establecimiento de rutas multi-salto entre nodos aleatorios, y por tanto facilita las pruebas a realizar de las técnicas propuestas en una red móvil ad-hoc. La distribución inicial de los nodos se escoge aleatoriamente (ver sección 4.3.3). El modelo de tráfico simula sesiones de descarga de páginas web basadas en el modelo usado en [29], con los parámetros ya explicados en 4.3.1. Para considerar posibles situaciones de congestión de tráfico, un total de 15% de nodos en promedio tienen una sesión activa de tráfico. La interfaz radio simulada corresponde al estándar 802.11a operando en la banda de frecuencia de 5.8GHz y transmitiendo con una nivel de potencia fija de 17dBm.

Se consideran los efectos de propagación radio realistas presentados en el capítulo 4 como las pérdidas de propagación, el desvanecimiento lento, y el desvanecimiento multitrayecto. En concreto se ha utilizado el modelo de canal urbano micro-celular propuesto en el proyecto WINNER [26], que diferencia entre visión directa (LOS) y no visión directa (NLOS). El trabajo presentado en [26] indica también que la desviación estándar del desvanecimiento lento debe ser igual a 3dB y a 4dB para condiciones de LOS y NLOS respectivamente. Se ha implementado el modelo Gudmunson para considerar las propiedades de la correlación del desvanecimiento. El efecto de desvanecimiento multitrayecto, que resulta de la recepción de múltiples réplicas de la señal transmitida en el receptor, se modela con una distribución de Ricean en condiciones de LOS y con una distribución de Rayleigh en condiciones NLOS.

La plataforma de simulación utilizada modela la capa MAC 802.11a basada en CSMA/CA (*Carrier Sense Multiple Access with Collision Avoidance*) y el modo de operación DCF (*Distributed Coordination Function*). La capa MAC modelada incluye

también el mecanismo RTS/CTS (*Request to Send/Clear to Send*). Para reducir la complejidad de las simulaciones a nivel de sistema, los efectos procedentes de la capa física que resultan de la naturaleza aleatoria del entorno radio se modelan por medio de Tablas LUT (*Look Up Tables*), siguiendo los resultados de [28]. Estas LUTs, extraídas de simulaciones a nivel de enlace, mapean la tasa de error de paquete PER (*Packet Error Rate*) con las condiciones de calidad de canal experimentadas.

La Tabla 6-1 resume los valores de los parámetros de configuración de las simulaciones llevadas a cabo en este capítulo.

Parámetro	Valor
Tipo escenario	Manhattan 6x6 edificios
Dimensiones	1350x1350 m^2
Modelo movilidad	*Random Walk Obstacle* [31]
Número nodos	238
Densidad lineal nodos	1 nodo cada 80m
Interfaz radio transmisiones ad-hoc	802.11a en banda de 5.8GHz
Potencia transmisión	Fijo 17dBm / Variable 14/17/20dBm
Modelo propagación canal radio	Urbano micro-celular WINNER [26]
Distinción propagación LOS/NLOS	Sí (ver sección 4.2.2)
Modelado capa MAC	CSMA/CA, DCF y RTS/CTS.
Modelado efectos de capa física	LUT de *Packet Error Rate* (PER)
Modelo tráfico	Tráfico web [29]
Porcentaje nodos con sesiones activas	Fijo 15% / Variable 15-65%
Porcentaje nodos egoístas	0/10/20/30/40%

Tabla 6-1 Configuración de parámetros de simulación.

6.4.3 Análisis comparativo

En este apartado se exponen y discuten los resultados de las simulaciones llevadas a cabo. Las técnicas Marti y TEAM sirven a la vez como técnicas de referencia en su implementación original con las cuales comparar las mejoras de rendimiento obtenidas, y también como soporte sobre el cual se implementan las técnicas propuestas en este capítulo. Se estudiarán los parámetros de medición de rendimiento expuestos en el apartado 6.4.1 reflejando las relaciones entre la variación en el número de acusaciones correctas e incorrectas, el número de negaciones y establecimientos de ruta, por un lado, y

por otro, los parámetros relacionados con la conectividad como el PDR o los porcentajes de paquetes perdidos por distintas causas.

Las Tablas 6-2 y 6-3 muestran la mejora obtenida al combinar las técnicas propuestas con las implementaciones originales de Marti y TEAM. WRAM se refiere al uso combinado de las técnicas WM y RAM. Los parámetros considerados (establecimientos de ruta, negaciones de ruta y acusaciones) fueron definidos en el apartado 6.4.1. Los resultados en las Tablas 6-2 y 6-3 corresponden a un escenario con un 20% de nodos egoístas. Los resultados obtenidos para otros porcentajes de nodos siguen tendencias similares, en el sentido en que se obtienen incrementos porcentuales similares.

Todas las técnicas propuestas son capaces de reducir significativamente el número de negaciones de ruta incorrectas. Más aún, existe una alta correlación entre la reducción del número de acusaciones incorrectas, la reducción del número de negaciones de ruta incorrectas, y la reducción en el porcentaje de paquetes perdidos por la no disponibilidad de rutas seguras (factor que será discutido más adelante). Las negaciones de ruta incorrectas reducen la disponibilidad de rutas seguras conocidas, y por tanto reducen la conectividad multi-salto y el PDR. Este efecto no deseado de las implementaciones originales de Marti y TEAM se contrarresta al reducir el número de acusaciones incorrectas. A pesar de que todas las técnicas propuestas reducen significativamente el número de acusaciones incorrectas, es importante subrayar la considerable reducción conseguida con WM y WRAM; en ambos casos, la reducción es mayor del 90%. En el caso de RAM, siempre que se detecta una acción cooperativa, la reputación del nodo retransmisor se restablece si había sido previamente degradada incorrectamente debido a la acumulación de observaciones incorrectas de acciones egoístas provocadas por errores de transmisión radio y colisiones de paquetes. Con WM, la introducción de la categoría "sospechoso" también contribuye a la reducción del número de acusaciones incorrectas. Como se comentó anteriormente, un alto porcentaje de nodos cooperativos dejarán de ser acusados incorrectamente al poder permanecer en la categoría de "sospechoso" y tener la oportunidad de volver a la de "cooperativo" cuando las condiciones de propagación mejoran. RFM también consigue una reducción del número de acusaciones incorrectas en las Tablas 6-2 y 6-3 al restaurar la reputación de los nodos retransmisores que sufren alguna caída de enlace, y es detectada por el nodo observador antes de que sea acusado de actuar egoístamente. Así se alivian los efectos negativos de las caídas de enlace sobre los niveles de reputación con la propuesta RFM. Por otro lado, resulta llamativa la reducción en el número de acusaciones correctas obtenido con WM (y WRAM) al emplearse junto con la técnica de Marti en la Tabla 6-2. Este efecto no es deseable, ya que la reducción en el número de acusaciones correctas conduce a un aumento del número de establecimientos de ruta incorrectos en la Tabla 6-2, que en definitiva podría aumentar el porcentaje de paquetes descartados por nodos egoístas. Sin embargo, se observará y

justificará posteriormente al evaluar este parámetro que la reducción en el número de acusaciones correctas experimentado por WM y WRAM en la Tabla 6-2 no tiene una repercusión negativa en el porcentaje de paquetes entregados PDR (Figuras 6-6 y 6-7).

	RFM	WM	RAM	WRAM
Acusaciones incorrectas [%]	-24.45	-91.39	-59.58	-97.01
Acusaciones correctas [%]	-3.35	-46.59	-6.57	-51.5
Establecimientos incorrectos de ruta [%]	2.47	45.92	-1.26	38.47
Establecimientos correctos de ruta [%]	14.19	47.49	26.38	39.46
Negaciones incorrectas de ruta [%]	-22.35	-76.51	-56.66	-94.27
Negaciones correctas de ruta [%]	-5.78	-6.81	-10.36	-17.67

Tabla 6-2 Mejora obtenida con las técnicas propuestas respecto a la técnica de Marti original.

	RFM	WM	RAM	WRAM
Acusaciones incorrectas [%]	-37.16	-62.96	-76.01	-92.47
Acusaciones correctas [%]	-7.82	-10.7	-7.54	-15.51
Establecimientos incorrectos de ruta [%]	5.3	24.8	-2.13	17.92
Establecimientos correctos de ruta [%]	9.48	24.18	20.43	24.5
Negaciones incorrectas de ruta [%]	-37.39	-73.48	-79.44	-95.22
Negaciones correctas de ruta [%]	-11.62	-24.32	-20.48	-34.67

Tabla 6-3 Mejora obtenida con las técnicas propuestas respecto a la técnica TEAM original.

Las Figuras 6-4 y 6-5 representan el porcentaje de paquetes perdidos debido a la no disponibilidad de rutas seguras, en función del porcentaje de nodos egoístas en el escenario. Los resultados que se obtienen aplicando las técnicas propuestas se comparan con las técnicas de Marti (Figura 6-4) y TEAM (Figura 6-5). Los términos TEAM y Marti en la leyenda de las figuras corresponden a los resultados obtenidos con su implementación original. Para mayor claridad, sólo se incluyen los resultados con WM, RAM, RFM y WRAM. Los números incluidos en las figuras indican la diferencia en el rendimiento entre la mejor de las propuestas (generalmente WRAM), y la correspondiente implementación original de Marti y TEAM. Es importante notar que el incremento de la disponibilidad de rutas multi-salto seguras resulta en una notable reducción del porcentaje de paquetes perdidos debido a la no disponibilidad de rutas.

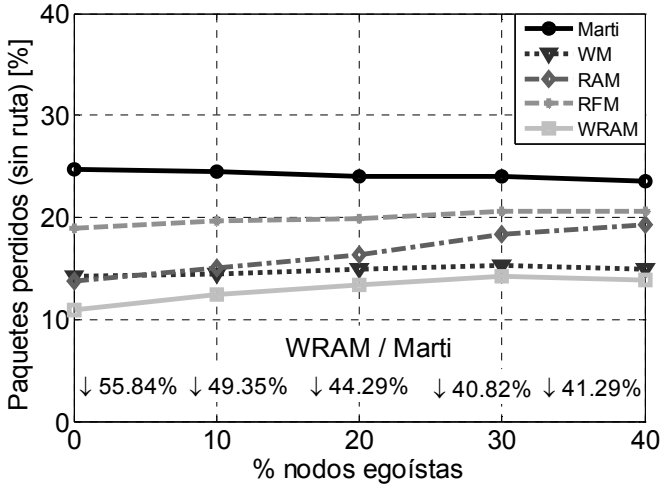


Figura 6-4. Porcentaje de paquetes perdidos sin ruta respecto a la técnica original de Marti.

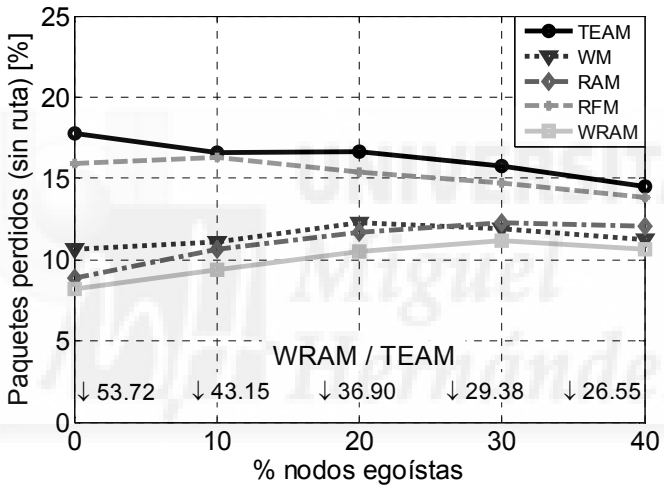


Figura 6-5. Porcentaje de paquetes perdidos sin ruta respecto a la técnica original TEAM.

Las Figuras 6-6 y 6-7 representan el PDR obtenido por las diferentes técnicas propuestas al ser aplicadas a Marti y a TEAM respectivamente. La capacidad para diferenciar a los nodos egoístas y cooperativos con las técnicas propuestas en este trabajo resulta en un notable incremento del PDR respecto a las técnicas de reputación originales. En las figuras puede apreciarse que este incremento se mantiene con pequeñas variaciones cuando varía el porcentaje de nodos egoístas. RAM consigue el mayor incremento de PDR cuando se aplica sobre Marti. Sin embargo, cuando se aplica sobre TEAM, WRAM consigue un incremento mayor. Los resultados en las Figuras 6-6 y 6-7 muestran que en general el incremento en PDR obtenido con las técnicas propuestas es mayor cuando se aplica sobre TEAM que cuando se aplica sobre Marti. Sin embargo, la reducción en el porcentaje de paquetes perdidos por la no disponibilidad de rutas seguras (Figuras 6-4 y 6-5) es mayor en la técnica de Marti que en TEAM. Esta aparente

contradicción se debe al hecho de que al combinar las técnicas propuestas con la técnica de Marti, hay un pequeño incremento de los paquetes perdidos debido a caídas de enlace (este efecto se comenta más adelante). Por otro lado, cuando las técnicas propuestas se combinan con TEAM, se consigue una pequeña reducción de los paquetes perdidos debido a caídas de enlace. Como se ha comentado, las Tablas 6-2 y 6-3 mostraban que las técnicas propuestas reducen el número de negaciones de ruta correctas, siendo además más significativas en el caso de las técnicas que usan el modo WM (WM y WRAM). Esto se debe al modo de funcionamiento de la categoría "sospechoso" en WM, que también reduce el número de acusaciones correctas. Aunque este no es un efecto deseable, las Figuras 6-6 y 6-7 muestran que en conjunto no tiene un impacto negativo en el PDR.

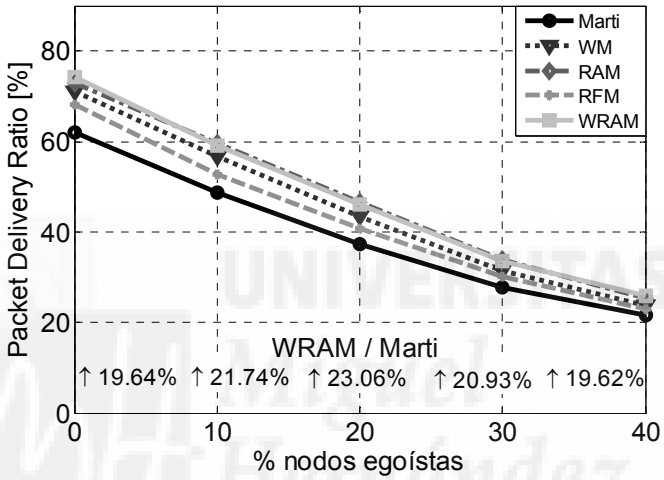


Figura 6-6. PDR obtenido con las técnicas propuestas respecto a la técnica original de Marti.

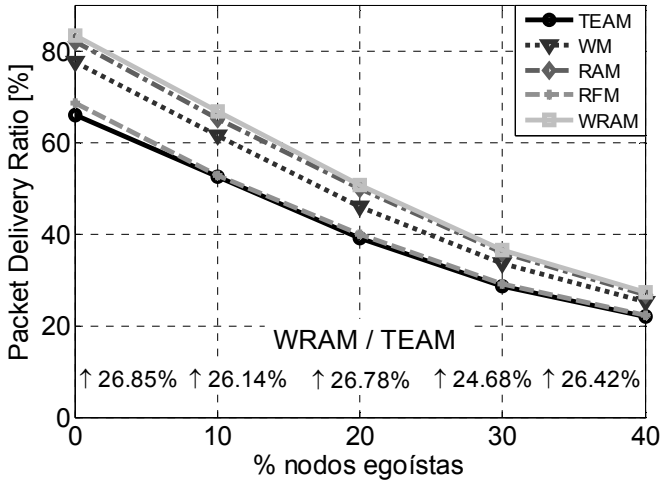


Figura 6-7. PDR obtenido con las técnicas propuestas respecto a la técnica original TEAM.

Los valores de PDR alcanzados no están influenciados únicamente por el porcentaje de paquetes perdidos debido a la no disponibilidad de rutas, sino también por el porcentaje de paquetes descartados por nodos egoístas (Figuras 6-8 y 6-9). Este parámetro está influenciado a su vez por una combinación de los parámetros de reputación mostrados en las Tablas 6-2 y 6-3. Al reducir el número de establecimientos de ruta incorrectos, o aumentar el número de establecimientos de ruta correctos, desciende el porcentaje de paquetes descartados por nodos egoístas. Además, incrementar el número de acusaciones correctas y el número de negaciones de ruta correctas también reduce el número de paquetes descartados por los nodos egoístas. RAM (y las combinaciones que incluyen RAM, como WRAM) es la única técnica que consigue reducir este parámetro en las Figura 6-8 y 6-9. Por ello, sólo las combinaciones que incluyen RAM consiguen reducir, o al menos incrementar sólo ligeramente, el porcentaje de paquetes descartados por los nodos egoístas. Esto es porque RAM es la única técnica que reduce el número de establecimientos de ruta incorrectos en las Tablas 6-2 y 6-3. Las demás técnicas, y en particular WM, incrementan el número de establecimientos de ruta incorrectos. Cuando un nodo es acusado de actuar egoístamente, WM rompe el enlace y marca el nodo en la categoría "sospechoso". A partir de entonces, las peticiones de ruta que vienen de nodos "sospechosos" no se rechazan con el fin de descartar la posibilidad de que la acusación realizada estuviera motivada por observaciones incorrectas de descartes. De esta forma, la propuesta WM incrementa el número de establecimientos de ruta incorrectos, pero también incrementa, pero sólo ligeramente, el porcentaje de paquetes descartados por nodos egoístas (Figuras 6-8 y 6-9). Esto es posible gracias a que la duración de las rutas con nodos egoístas es más corta cuando han sido categorizados como "sospechosos", ya que serán vigilados más estrechamente que los nodos "neutrales". De esta manera, si un nodo "sospechoso" está actuando egoístamente, una observación de descarte más será suficiente para acusarlo definitivamente, lo cual a su vez reduce el impacto de incrementar el número de establecimientos de ruta incorrectos sobre el porcentaje de paquetes descartados por nodos egoístas. La propuesta RFM también incrementa ligeramente los paquetes descartados por nodos egoístas en las Figuras 6-8 y 6-9 debido al pequeño incremento en el número de rutas incorrectas establecidas, y a la reducción del número de negaciones de ruta correctas (ver Tablas 6-2 y 6-3). Esto es debido a la restauración de la reputación realizada por RFM en caso de caídas de enlace. En algunas ocasiones, la reputación de un nodo egoísta es restaurada debido a la caída del enlace, si el nodo no ha sido todavía categorizado como egoísta. Sin embargo, el incremento en el porcentaje de paquetes descartados por nodos egoístas en el caso de RFM es inferior a un 3% en las Figuras 6-8 y 6-9. Por consiguiente, la mayoría de los nodos egoístas son detectados antes de que ocurra una caída de enlace. Para disminuir el número de paquetes descartados por nodos egoístas en RFM y WM, sería necesario hacer que las técnicas de reputación fueran menos tolerantes a los descartes de paquetes, por ejemplo reduciendo el

tiempo de expiración o reduciendo el número máximo de faltas, pero esto debe hacerse con cuidado puesto que podría acabar aumentando el número de acusaciones incorrectas y por tanto reduciendo el número de rutas seguras conocidas.

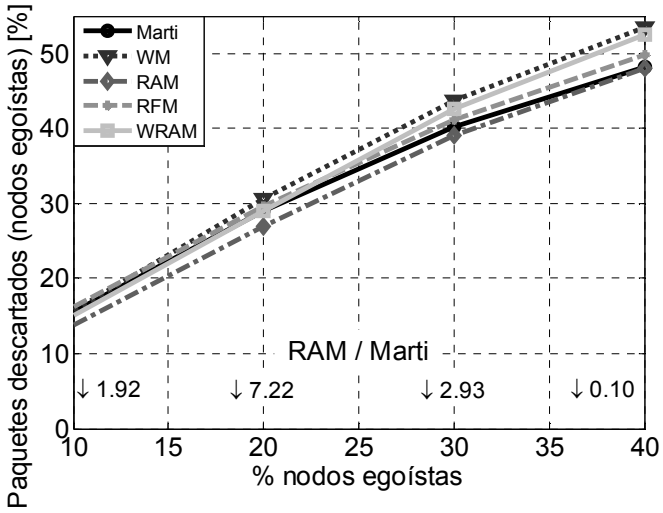


Figura 6-8. Porcentaje de paquetes descartados por nodos egoístas respecto a la técnica original de Marti

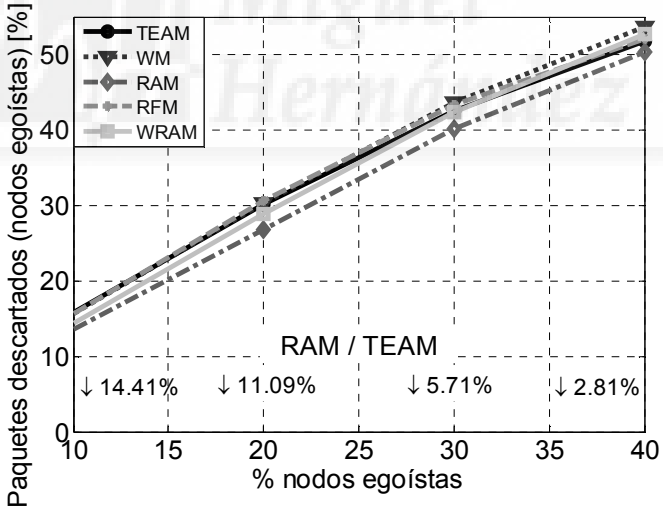


Figura 6-9. Porcentaje de paquetes descartados por nodos egoístas respecto a la técnica original TEAM

Otro de los factores que tienen influencia sobre el rendimiento del PDR en las Figuras 6-6 y 6-7 es el porcentaje de paquetes perdidos debido a caídas de enlace, que se muestra en las Figuras 6-10 y 6-11. La capa MAC de 802.11 realiza las funciones de coordinación de acceso al canal radio compartido entre los diferentes nodos móviles mediante el protocolo DCF. En redes radio, un nodo transmisor no puede escuchar colisiones en el

canal mientras está transmitiendo él mismo, ni tampoco puede escuchar el canal. Por ello, el nodo receptor debe enviar un ACK si ha recibido la trama sin ningún error. Si el transmisor no recibe un ACK después de un período de tiempo específico, asume que la transmisión no se ha realizado correctamente debido a colisiones de paquetes o a errores de transmisión radio, y retransmite la trama. Cuando se alcanza el número máximo de retransmisiones establecido, la MAC del nodo transmisor descarta el paquete e informa a las capas superiores de la caída del enlace. El protocolo de enrutamiento deshace la ruta e inicia un nuevo proceso de descubrimiento de ruta si es necesario. Las Figuras 6-10 y 6-11 muestran que el porcentaje de paquetes descartados por caídas de enlace es mayor para Marti que para TEAM. Es más, la Figura 6-11 muestra que cuando las técnicas propuestas se aplican a TEAM, el porcentaje de paquetes perdidos decrece en comparación con la implementación original; por otro lado, ocurre lo contrario para la técnica Marti en la Figura 6-10. Las condiciones que los paquetes empleados para el procedimiento de búsqueda de rutas (mensajes RREQ) deben cumplir para poder ser retransmitidos por los nodos intermedios encargados de buscar la ruta, son más estrictas en TEAM que en Marti (capítulo 5). La técnica de Marti sólo rechaza un paquete de búsqueda de ruta cuando se detecta un nodo egoísta en la ruta. En cambio, cuando un nodo recibe un paquete de búsqueda de ruta, TEAM evalúa si la reputación media de los nodos que participan en la ruta es mayor que el límite de reputación establecido. Por ello, en la técnica de Marti se retransmiten un número mayor de mensajes RREQ en comparación con la técnica TEAM. La sobrecarga de enrutamiento generada por Marti resulta en un incremento de la utilización del canal de comunicación, y por tanto en la pérdida de tramas de datos MAC como consecuencia de las colisiones de paquetes.

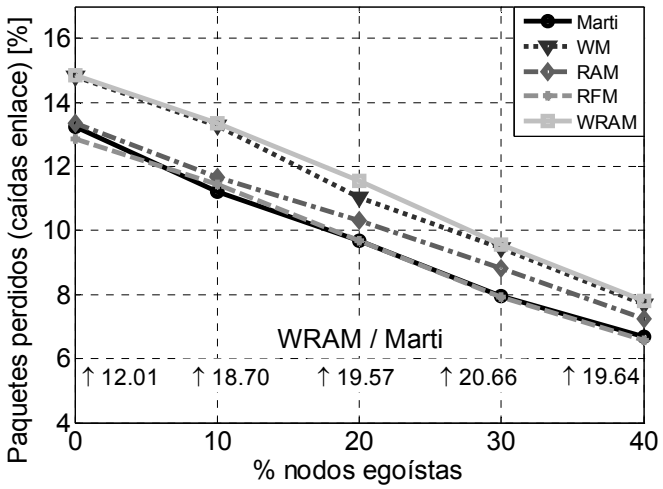


Figura 6-10. Porcentaje de paquetes perdidos por caídas de enlace respecto la técnica de Marti.

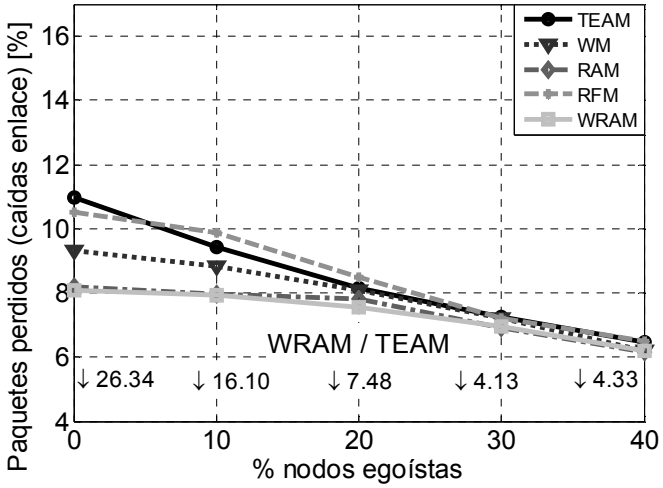


Figura 6-11. Porcentaje de paquetes perdidos por caídas de enlace respecto a la técnica TEAM.

El agente TEAM en cada nodo retransmisor evalúa la reputación de cada paquete de datos que debe retransmitir. Si la reputación del paquete es menor que el límite umbral establecido, el paquete es descartado por su origen no seguro (ver apartado 5-4). Como era de esperar, la reducción en el número de acusaciones incorrectas, y también en el número de acusaciones correctas (ver Tabla 6-3) resulta en una importante reducción del porcentaje de paquetes descartados por su origen no seguro (Figura 6-12). Esto también beneficia al incremento del PDR conseguido con las técnicas propuestas aplicadas sobre TEAM en la Figura 6-7.

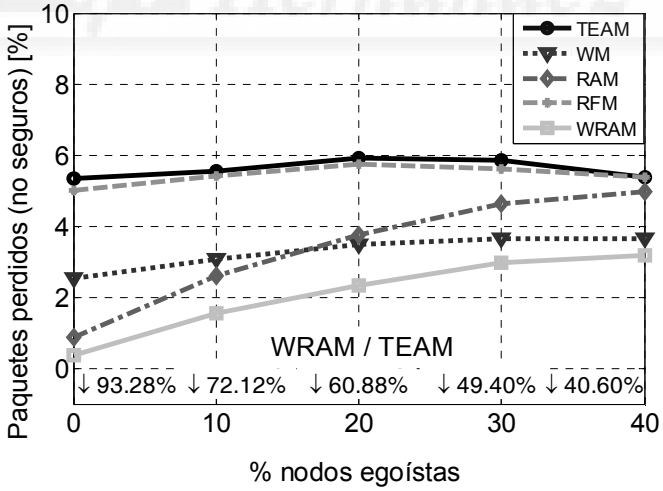


Figura 6-12. Porcentaje de paquetes descartados por origen no seguro respecto a la técnica TEAM.

Las Figuras 6-13 a 6-16 muestran el efecto de la variación del porcentaje de errores de transmisión radio sobre los principales parámetros de rendimiento. Las figuras comparan el rendimiento obtenido por las propuestas WM, RAM, RFM y WRAM al ser aplicadas sobre las técnicas originales de Marti y TEAM[33]. El porcentaje de error de transmisión radio, ha sido modificado variando el nivel de potencia de transmisión, que ha tomado los valores 14dBm, 17dBm y 20dBm. El error de transmisión radio se representa en el eje de ordenadas derecho en las Figuras 6-13 a 6-16. Incrementar la potencia de transmisión reduce el porcentaje de errores de transmisión radio, y aumenta el rango de comunicación de los nodos. Por consiguiente, el número medio de saltos por ruta decrece, y por tanto hay un porcentaje menor de paquetes descartados sin ruta, como se aprecia en la Figura 6-15. Esto se debe a que cuando el número de saltos por ruta es menor, aumenta la probabilidad de encontrar rutas seguras, como se vio en el capítulo 5. Esto conlleva una mejora significativa del PDR con todas las técnicas al aumentar la potencia de transmisión. Igual que ocurre con el escenario de referencia (potencia de transmisión de 17dBm), sólo la técnica RAM es capaz de reducir el número de paquetes descartados por nodos egoístas en la Figura 6-16. Sin embargo, todas las técnicas propuestas son capaces de mejorar el PDR respecto a la técnica de reputación original, siendo además mayor la mejora cuanto menor es la potencia de transmisión (y por tanto, mayores errores de transmisión radio se producen).

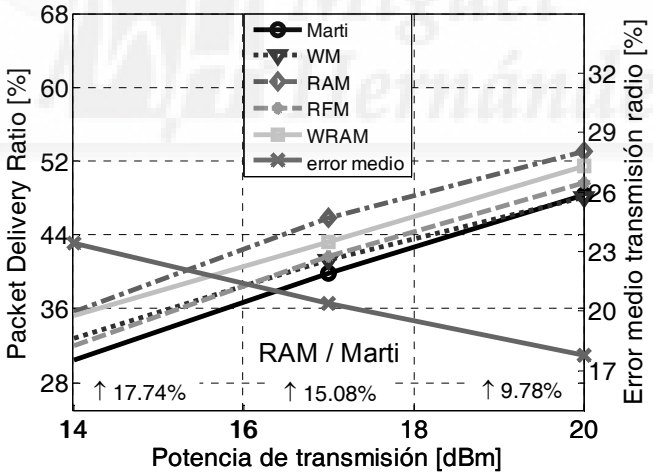


Figura 6-13. PDR de las técnicas con Marti para distintos niveles de error de transmisión radio.

[33] Las figuras muestran el incremento máximo que se puede obtener por las técnicas propuestas, así como el porcentaje medio de errores de transmission radio por cada nivel de potencia.

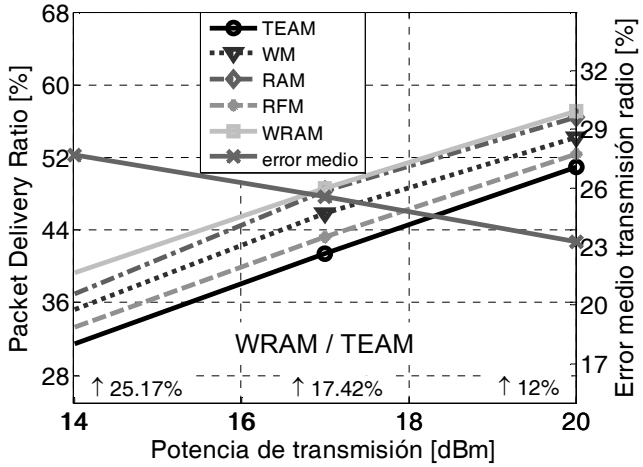


Figura 6-14. PDR de las técnicas con TEAM para distintos niveles de error de transmisión radio.

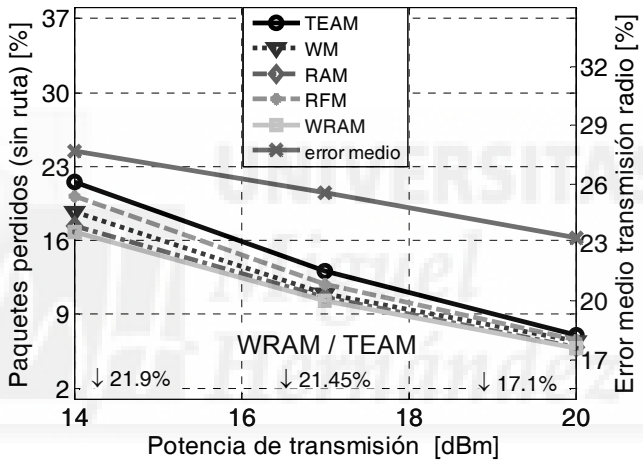


Figura 6-15. Paquetes perdidos sin ruta para distintos niveles de error de transmisión radio.

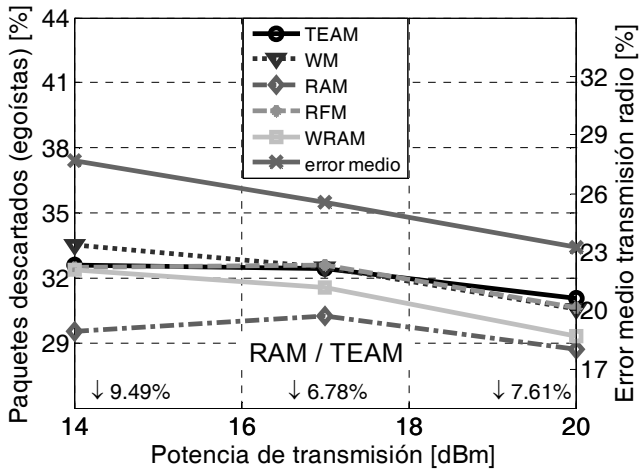


Figura 6-16. Paquetes descartados por egoístas para distintos niveles de error de transmisión radio.

También se ha analizado el efecto de variar el porcentaje de colisiones de paquete, es decir, el porcentaje de ocasiones en que los paquetes MAC eran descartados por haberse producido una colisión en el momento de su recepción. Para modificar este porcentaje, se ha variado la razón de sesiones activas de usuario simultáneas desde un 15% (que constituye el caso de referencia) hasta un 65%. Para ello, se redujo el intervalo medio entre el inicio de sesiones, dado que el número de usuarios no se varió. El eje *y* derecho en las figuras 6-17 a 6-22 corresponde a la tasa de paquetes perdidos por colisiones, en porcentaje. Los resultados obtenidos muestran que al aumentar el porcentaje de sesiones activas (y como consecuencia de la tasa de colisiones de paquetes) se incrementa el número de paquetes descartados sin ruta en la Figura 6-19 (se representa la técnica TEAM pero los resultados para Marti son equivalentes) y desciende el PDR (Figuras 6-17 y 6-18, que muestran el PDR para Marti y para TEAM respectivamente), especialmente cuando se utilizan las implementaciones originales de las técnicas de Marti y TEAM. Sin embargo, todas las técnicas propuestas (en particular, WRAM y RAM) reducen considerablemente el porcentaje de paquetes perdidos sin ruta en comparación con las técnicas de Marti y TEAM originales. La reducción es mayor cuando aumenta la tasa de colisiones de paquetes. Al aumentar el porcentaje de sesiones activas de usuario se reduce el número de paquetes descartados por nodos egoístas (Figura 6-20). Esto es debido a que cuando los nodos usan con mayor frecuencia el canal de comunicación, aprenden más fácilmente la identidad de los nodos egoístas. Por consiguiente, el número de establecimientos de ruta incorrectos disminuye (y el número de negaciones correctas de ruta aumenta), como puede verse en las Figura 6-21 y 6-22. La Figura 6-21 muestra el número de establecimientos de ruta con nodos egoístas (normalizado por el porcentaje de sesiones activas de usuario para hacer una comparación justa) con la técnica TEAM y las técnicas propuestas. La Figura 6-22 muestra el número de negaciones correctas.

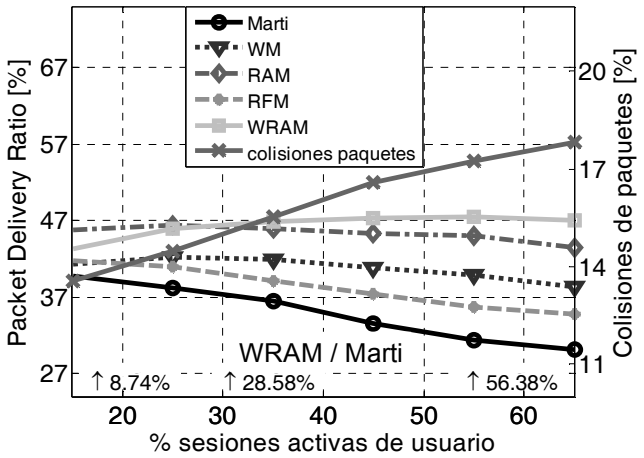


Figura 6-17. PDR de las técnicas con Marti para distintas tasas de colisiones de paquetes.

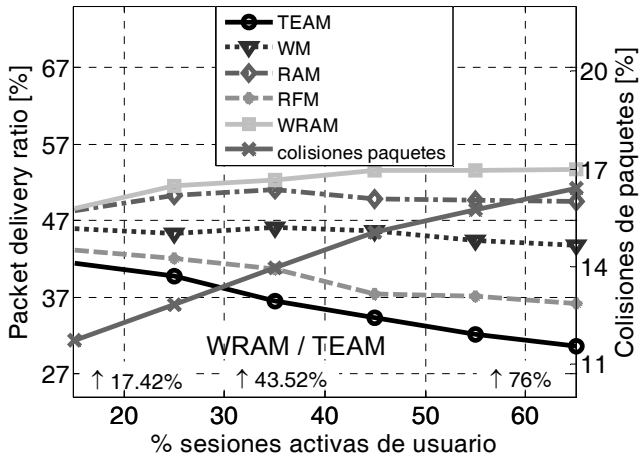


Figura 6-18. PDR de las técnicas con TEAM para distintas tasas de colisiones de paquetes.

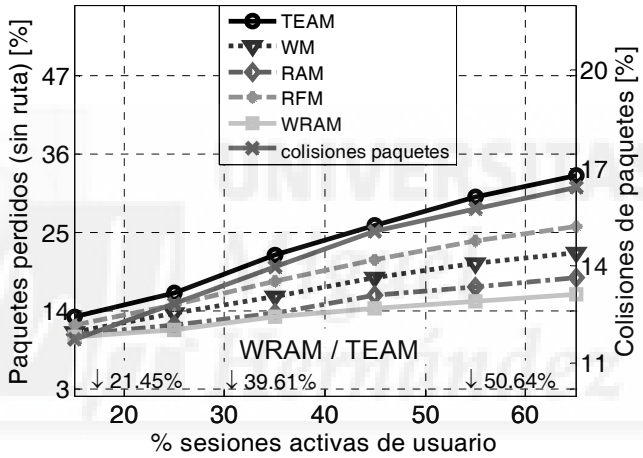


Figura 6-19. Paquetes perdidos sin ruta para distintas tasas de colisiones de paquetes.

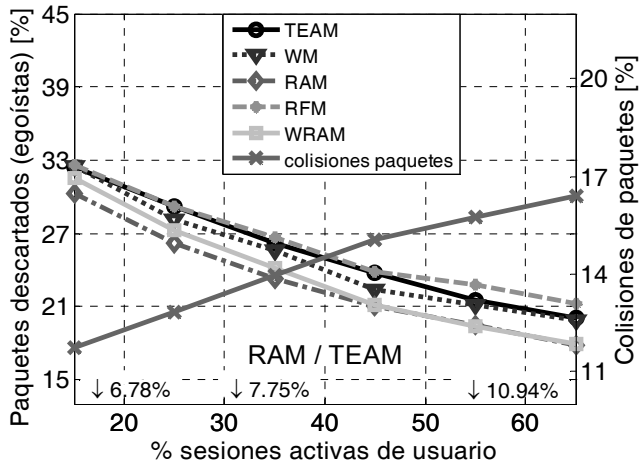


Figura 6-20. Paquetes descartados por nodos egoístas para distintas tasas de colisiones de paquetes

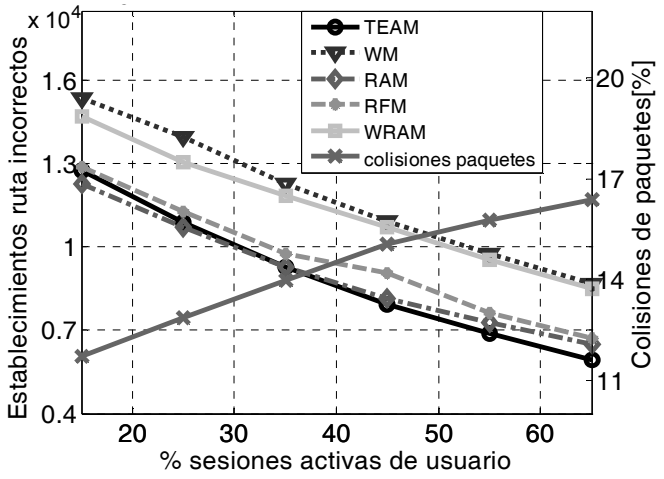


Figura 6-21. Número de establecimientos de ruta incorrectos con las técnicas propuestas respecto a TEAM para diferentes tasas de colisiones de paquetes

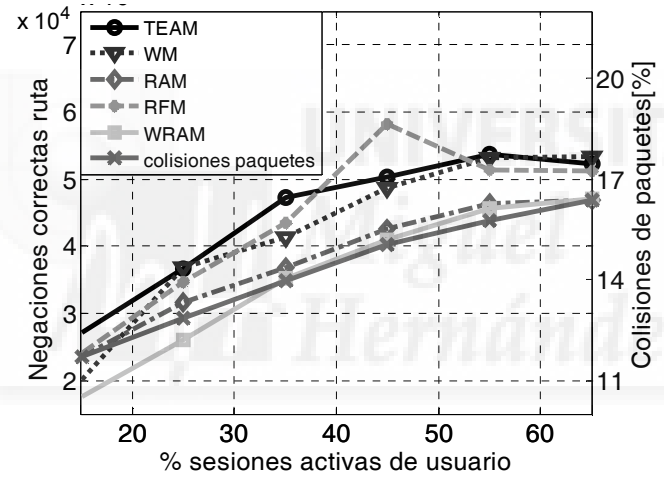


Figura 6-22. Número de negaciones correctas de ruta con las técnicas propuestas respecto a TEAM para diferentes tasas de colisiones de paquetes

Para finalizar, es necesario recalcar que los resultados obtenidos muestran que las mejoras obtenidas con WRAM con respecto a Marti y TEAM en términos de tasa de entrega de paquetes (PDR) se incrementan al aumentar el porcentaje de sesiones activas de usuario (Figuras 6-17 y 6-18). Esto es debido a que conforme aumenta el porcentaje de usuarios activos, el número de paquetes descartados por nodos egoístas disminuye (Figura 6-20), y sólo se da un ligero incremento en el número de paquetes perdidos sin ruta (Figura 6-19).

6.5 Conclusiones

Tras haber constatado en el capítulo 5 que el rendimiento de técnicas de reputación tales como Marti y TEAM podía degradarse al ser evaluado experimentalmente en condiciones realistas, en el presente capítulo se han propuesto tres técnicas que tratan de mitigar dicha degradación. Parte del deterioro experimentado proviene en realidad del error en el proceso de observación de la retransmisión de los paquetes introducido por la técnica *watchdog*. Este error, tal y como fue comprobado en el capítulo anterior, estaba provocado por errores de propagación radio y colisiones de paquetes que impedían que el nodo observador escuchara correctamente la retransmisión. Este efecto se acrecienta en condiciones realistas de simulación, considerando modelos de canal precisos y también al aumentar la carga de tráfico de usuario. La principal consecuencia que los mecanismos propuestos tratan de combatir es el hecho de que las técnicas como Marti y TEAM, al procesar esta información errónea proveniente del *watchdog*, lo reproducen al acusar incorrectamente a nodos que en realidad no son egoístas, descartando potenciales rutas seguras, aislando a nodos cooperativos, y en definitiva, limitando su capacidad para encontrar rutas fiables.

Las estrategias propuestas en este capítulo tienen como objetivo compensar la inexactitud de *watchdog* y rebajar el nivel de acusaciones incorrectas para mejorar la conectividad de las redes MANET. Cada una de las propuestas encara el problema desde un ángulo diferente. RAM magnifica la importancia de las retransmisiones observadas correctamente, dado que sirven para confirmar las retransmisiones que estén pendientes de ser observadas, y también restaurar la reputación del nodo que haya podido ser degradada injustamente. RFM combate la disminución de reputación que pueden provocar las caídas del enlace radio. Por último, WM introduce una categoría intermedia entre la de nodo cooperativo y nodo sospechoso, que proporciona una oportunidad más al nodo para distinguir las acusaciones correctas a nodos egoístas, de las acusaciones incorrectas a nodos cooperativos provocadas por la inexactitud de *watchdog*.

Los resultados obtenidos han demostrado la capacidad de las técnicas propuestas para reducir el número de acusaciones incorrectas, e incrementar la disponibilidad de rutas multi-salto seguras, lo cual ha propiciado un aumento del PDR en redes MANET en presencia de nodos egoístas. Se ha observado también un efecto no deseado que consiste en una reducción del número de acusaciones correctas en ciertos casos concretos. Esto podría provocar un aumento del número de rutas con nodos egoístas que son utilizadas por los nodos para retransmitir sus paquetes. Los paquetes encaminados a través de estas rutas serían descartados por los nodos egoístas, reduciendo el PDR. Sin embargo, los resultados obtenidos muestran que la reducción en el número de acusaciones correctas sólo es apreciable cuando se aplica sobre la técnica más simple, la de Marti, y cuando se

combina con la técnica WM. En este caso, la disminución en el número de acusaciones incorrectas provocado por la técnica WM se debe a que muchos de esos nodos egoístas, en lugar de ser acusados, son señalados como sospechosos y apartados de la comunicación si no vuelven a cooperar. Posteriormente pueden ser detectados y aislados si vuelven a participar en el enrutamiento de paquetes. Aunque no son acusados en primera instancia, sí son apartados de la comunicación y aislados. Por esta razón, los nodos egoístas detectados como sospechosos no tienen ocasión de descartar más paquetes. Esto explica la mínima incidencia de este efecto sobre el PDR. Por eso, incluso en este caso el PDR final aumenta, dado que prevalece el efecto de la mayor disponibilidad de rutas seguras.

A pesar del buen funcionamiento de las técnicas propuestas mostrado en este capítulo, cabe señalar que la asunción de que el comportamiento egoísta de los nodos es continuo puede no ser aplicable a todas las situaciones. Algunos nodos egoístas, dada la incertidumbre que la calidad del canal radio introduce en el proceso de observación de *watchdog*, pueden aprovecharla para disminuir el número de paquetes que retransmiten para los demás nodos y pasar desapercibidos al mismo tiempo. Por ello, algunos estudios asumen nodos egoístas que son capaces de descartar no todos los paquetes que deben retransmitir, sino sólo una fracción de ellos, de manera aleatoria, para simular el efecto de un canal radio de baja calidad. En tal caso, algunas de las técnicas propuestas para mejorar el rendimiento en este capítulo podrían no dar el resultado deseado, ya que los nodos podrían escapar a la detección, pues este comportamiento es más difícil de detectar, al confundirse con la imprecisión de *watchdog*. Por todo ello, en el capítulo siguiente la asunción sobre el grado de egoísmo de los nodos se ampliará, para abarcar también a aquellos nodos que no descartan todos los paquetes. Esto exigirá replantear los criterios para decidir si un nodo debe ser acusado de comportamiento egoísta o no.

7

Detección Bayesiana y exponencial

En los capítulos anteriores se ha evaluado el rendimiento de distintas técnicas de incentivo a cooperación basadas en reputación que empleaban como método de observación la técnica *watchdog*. *Watchdog* es una técnica fácil de implementar y ampliamente utilizada por distintas técnicas basadas en reputación. Sin embargo, el capítulo 5 mostró la importancia de una evaluación en condiciones realistas del rendimiento y el funcionamiento de *watchdog*, y por extensión, de las técnicas de reputación que lo utilizan. Se mostró que las condiciones del canal de propagación tienen una notable influencia en la probabilidad de error de *watchdog*, es decir, en la probablidad de que *watchdog* tome una acción cooperativa como una acción egoísta. La incertidumbre introducida por el error de *watchdog* en el proceso de observación dificulta considerablemente el funcionamiento de las técnicas de reputación. Específicamente, el error de *watchdog* aumenta el número de acusaciones incorrectas, y paralelamente disminuye el número de rutas multi-salto disponibles. Este fue el punto de partida del capítulo 6, en el que se propusieron técnicas orientadas a mejorar estos aspectos. Los resultados han mostrado que estas técnicas conseguían mejorar la conectividad de la red al contrarrestar los efectos del error de *watchdog* sobre el número de acusaciones incorrectas.

Sin embargo, hasta ahora se había asumido que los nodos egoístas descartaban siempre los paquetes que debían retransmitir. Esta asunción puede no darse siempre. Algunos trabajos consideran que los nodos tienen un comportamiento aleatorio, en el que retransmitir o no un paquete depende de cierta probabilidad, la probabilidad de descarte [38] (ver sección 2.1.1). Este modelo con comportamiento aleatorio es una generalización del modelo de nodo egoísta considerado hasta ahora, en el que el nodo descartaba todos los paquetes. Con el modelo aleatorio de nodo egoísta resulta aún más dificultosa la tarea de detección de los nodos, dado que el comportamiento egoísta del nodo puede estar enmascarado por la probabilidad de error de *watchdog*. En tal caso, distinguir con precisión si un nodo está descartando paquetes o no puede requerir realizar una gran cantidad de observaciones. Por otro lado, cuanto mayor sea el número de observaciones requerido, mayor será también el número de paquetes que el nodo habrá descartado en caso de que efectivamente sea egoísta. De todo esto se deduce que, en el modelo probabilístico de nodo egoísta, existe un compromiso entre la velocidad y la precisión del proceso de observación [138]. Para robustecer el proceso de detección, es decir, hacerlo menos sensible al error introducido por la técnica de osbervación, los trabajos anteriores basan su decisión en un enfoque Bayesiano ([38],[48],[49],[50]), que requiere un número elevado de observaciones para reducir la probabilidad de acusar incorrectamente a un nodo cooperativo o de no detectar un nodo egoísta. En este contexto, este capítulo presenta un novedoso mecanismo de detección exponencial que supera las técnicas Bayesianas en rapidez y precisión. En primer lugar, se presenta el concepto de detección Bayesiano así como las distintas variantes basadas en este enfoque. Se analiza su funcionamiento y cómo aparece el compromiso mencionado. A continuación, se presenta la técnica exponencial y las principales diferencias con las técnicas Bayesianas. Finalmente, se evalúa el rendimiento de ambas en distintos escenarios de simulación.

7.1 Técnicas de detección Bayesianas

7.1.1 Descripción y variantes

Considérese una red MANET en la que algunos de los nodos no retransmiten los paquetes procedentes de otros nodos con probabilidad p_s. p_s es una variable aleatoria con una función de densidad de probabilidad desconocida $f_{ps}(x)$. Sea p_e la probabilidad de error de observación, es decir, la probabilidad de que la técnica de observación confunda una acción cooperativa con una acción egoísta. En *watchdog*, p_e equivale a la probabilidad de error de paquete debida a errores de transmisión radio y colisiones de paquetes. Se define D como el experimento aleatorio de la observación de la retransmisión con dos posibles resultados: D=0 si se observa una retransmisión, D=1 en

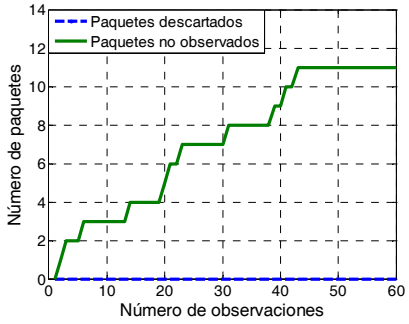
otro caso. Existen dos razones por las que la retransmisión puede no ser observada: el nodo descarta el paquete, con probabilidad p_s, o bien la retransmisión se realiza pero no se observa, con probabilidad $(1-p_s)p_e$. Este proceso se repite con cada paquete transmitido, conformando un proceso binomial D_n con probabilidad p_d:

$$\Pr(D=1) = p_s + (1-p_s)p_e = p_d \tag{7-1}$$

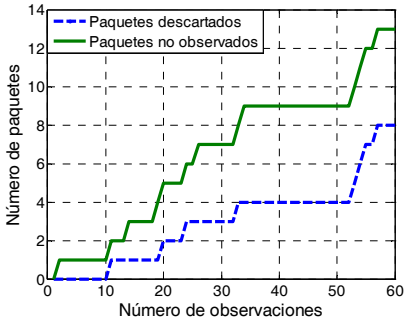
Tras cada observación debe evaluarse si el nodo está actuando egoístamente ($p_s>0$). En lo sucesivo, el proceso de decisión tras cada salida del proceso de observación de si un nodo está actuando o no egoístamente, se ha denominado proceso de detección. Esta decisión debe ser precisa para minimizar la tasa de acusaciones incorrectas[34] (*IA*, *Incorect Accusations*) y de no acusaciones incorrectas (*INA*, *Incorect No Accusations*), y rápida para que el número de acciones egoístas δ antes de que el nodo sea detectado sea también minimizado.

La Figura 7-1 muestra 4 ejemplos de muestras concretas del proceso aleatorio de observación de las retransmisiones. Las curvas representan dos parámetros: el número de paquetes descartados por el nodo egoísta, y el número de paquetes no observados (paquetes que el nodo precursor registra como no retransmitidos). En cada una de las figuras se consideran condiciones diferentes del proceso de observación, en cuanto al valor de los parámetros p_s y p_e. En las dos primeras, 7-1(a) y 7-1(b), el valor total del parámetro p_d es similar (0.2 y 0.19 respectivamente), y por tanto, el número total de paquetes no observados podría ser similar en ambos casos. Sin embargo, ambas corresponden a situaciones completamente diferentes: mientras en la Figura 7-1(a) el nodo retransmisor es un nodo cooperativo que no ha descartado ningún paquete ($p_s=0$), en la Figura 7-1(b) el nodo retransmisor ha realizado un total de 8 acciones egoístas tras 60 observaciones. Por otro lado, en las Figuras 7-1(c) y 7-1(d) se considera un mismo valor de p_d ($p_d = 0.86$). Sin embargo hay otra vez una divergencia notable entre los valores de p_s y p_e, y por tanto ambas situaciones podrían requerir diferentes reacciones por parte de la técnica de reputación correspondiente. Esto pone de relieve una cuestión importante: el proceso de detección requiere una aproximación del valor del parámetro p_e del proceso de observación. Cuanto mejor sea esta aproximación, mayor será la precisión del proceso de detección. En esta contribución, se asumirá que todas las técnicas de detección disponen de una misma herramienta para calcular la aproximación del valor de p_e con el fin de que puedan ser comparadas en igualdad de condiciones. El impacto de posibles desviaciones del valor del p_e estimado del p_e real serán estudiados en el apartado 7.3.4.

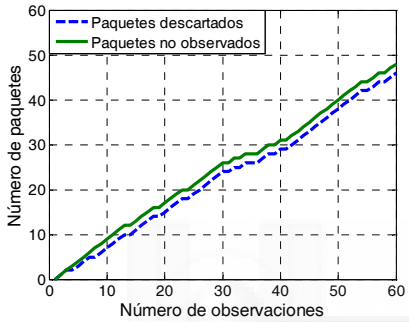
[34] *IA* se define como el cociente entre el número de nodos cooperativos acusados incorrectamente y el total de nodos cooperativos. *INA* se define como el cociente entre el número de nodos egoístas no acusados y el total de nodos egoístas. *IA* sólo es aplicable a nodos cooperativos mientras, que *INA* sólo puede aplicarse a nodos egoístas.



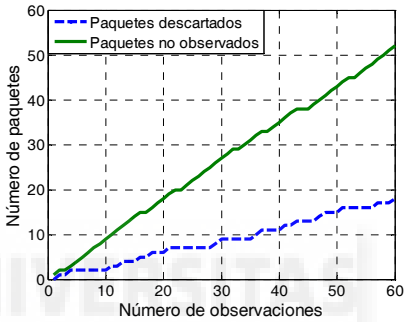
(a) $p_s = 0$, $p_e = 0.2$, $p_d = 0.2$



(b) $p_s = 0.1$, $p_e = 0.1$, pd = 0.19



(c) $p_s = 0.8$, $p_e = 0.3$, $p_d = 0.86$



(d) $p_s = 0.3$, $p_e = 0.8$, $p_d = 0.86$

Figura 7-1. Muestras del proceso aleatorio de observación de las retransmisiones.

Los mecanismos de detección más extendidos en la literatura son variantes del enfoque Bayesiano propuesto en [50]. [50] propone una métrica del egoísmo basada en la razón entre el número de acciones egoístas y cooperativas observadas (α y β). Tras cierto número de observaciones, se compara la métrica con un umbral para decidir si el nodo actúa egoístamente. Se han propuesto diferentes variantes basadas en este procedimiento. La primera, denominada aquí BIW (*Bayesian with Infinite Window*) [5], define la métrica como:

$$M_{BIW}(n,\alpha,l) = \left.\frac{\alpha_n}{n}\right|_{n \geq l} \tag{7-2}$$

donde α_n es el número de acciones egoístas registradas en las últimas n observaciones. n varía entre l y N, siendo l el número mínimo de observaciones requeridas antes de que se pueda tomar la primera decisión y N el máximo número de observaciones antes de que finalice la conexión. La segunda métrica, denominada BFW (*Bayesian with Finite Window*) y utilizada en [38] o [49], no considera todas las observaciones sino únicamente las últimas l, y se define como:

$$M_{BFW}(n,\alpha,l) = \left.\frac{\alpha_{n-l,n}}{l}\right|_{n\geq l} \tag{7-3}$$

La razón de considerar únicamente una ventana de las últimas l observaciones es otorgar más importancia a las observaciones más recientes. De esta manera, se prima que los nodos mantengan la cooperación a lo largo del tiempo, y al mismo tiempo un comportamiento correcto sostenido en el pasado no permite al nodo relajarse en el presente. Además facilita que los nodos puedan reaccionar más rápidamente a un cambio de comportamiento de un nodo egoísta. Siguiendo el mismo objetivo de otorgar mayor importancia a las observaciones recientes, [50] propone una métrica adicional, denominada BDF (*Bayesian with Discount Factor*), que introduce un factor de descuento u. El factor u representa la relación entre la importancia otorgada a las observaciones anteriores y la importancia del resultado de la observación más reciente, representada por s, tal y como expresa la siguiente ecuación:

$$\begin{aligned} \alpha_i &= u\alpha_{i-1} + s \\ \beta_i &= u\beta_{i-1} + (1-s) \end{aligned} \tag{7-4}$$

La ecuación 7-4 muestra el procedimiento de actualización de los parámetros α y β en la métrica BDF. Puede observarse cómo α y β no son simplemente la suma del número de comportamientos egoístas y cooperativos respectivamente como en la métrica Bayesiana más simple, sino que son la suma ponderada por el factor de descuento u de las observaciones anteriores y la observación actual. La métrica de egoísmo de BDF se calcula según la siguiente expresión:

$$M_{BDF}(n,\alpha,\beta,l) = \left.\frac{\alpha_n}{\alpha_n + \beta_n}\right|_{n\geq l} \tag{7-5}$$

Para escoger el valor del parámetro u, los autores proponían la siguiente regla del pulgar:

$$u = 1 - \frac{1}{m} = 1 - \frac{1}{l} \tag{7-6}$$

donde m es el número de observaciones que se considera suficiente para poder tomar una decisión sobre el egoísmo del nodo retransmisor con validez estadística. En el presente estudio, m coincide con el parámetro l que se ha definido anteriormente.

Además, se puede definir una variante que combine las dos anteriores: ventana finita y factor de descuento, denominada BFWDF (*Bayesian Finite Window with Discount Factor*). En esta técnica, por un lado se toman en cuenta únicamente las últimas l

observaciones. Por otro, ante cada nueva observación, con resultado *s*, se descarta la observación más antigua (para seguir considerando únicamente *l* observaciones) y se calcula el nuevo valor de α y β a partir de la expresión 7-4. La expresión para el cálculo de esta métrica es el siguiente:

$$M_{BFWDF}(n,\alpha,\beta,l) = \left.\frac{\alpha_{n-l,n}}{\alpha_{n-l,n}+\beta_{n-l,n}}\right|_{n\geq l} \tag{7-7}$$

7.1.2 Análisis por cadenas de Markov

Para el correcto funcionamiento de las técnicas Bayesianas es necesario seleccionar adecuadamente el valor de los parámetros de configuración *l* y τ para maximizar la precisión y la rapidez del proceso de detección. τ es el umbral de acusación que se compara con el valor de la métrica: si su valor es sobrepasado, el nodo es acusado. En la literatura no se ha encontrado ninguna aclaración sobre el procedimiento de selección, que depende además de los parámetros $f_{ps}(x)$ (la distribución del parámetro p_s entre los nodos de la red) y p_e. Aunque el valor de p_e puede ser estimado para cada conexión ([51] o [52]), la estimación de la función $f_{ps}(x)$ es difícil. Además, puede requerirse un gran número de observaciones para reducir la imprecisión, aumentando el número de paquetes descartados por los nodos egoístas. δ se define como el número de paquetes que un nodo descartada antes de ser detectado.

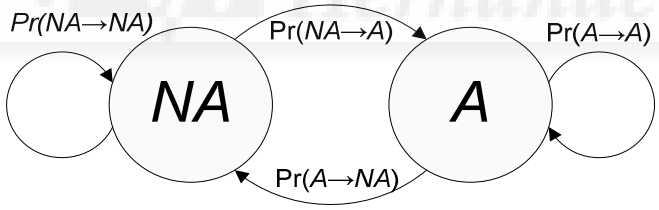


Figura 7-2. Diagrama del modelo de cadenas de Markov del proceso de detección.

Para entender mejor la importancia de los parámetros (τ,*l*), se analiza su influencia sobre las tasas *IA* e *INA* de manera analítica para la técnica BFW[35]. Si se considera un gran número de experimentos, el promedio de *IA* e *INA* puede ser aproximado a la probabilidad de que un nodo cooperativo sea acusado de actuar egoístamente y a la probabilidad de que un nodo egoísta no sea acusado. Considérese un modelo basado en cadenas de Markov para el método de detección BFW con dos posibles estados: acusación (*A*) y no acusación (*NA*) (ver Figura 7-2).

[35] Se escoge esta métrica por su simplicidad para el desarrollo analítico con cadenas de Markov.

Los estados iniciales A_l y NA_l representan la probabilidad de que, tras las primeras l observaciones, el número de acciones egoístas observadas α_l sea tal que la métrica BFW α_l/l resulte superior (o inferior respectivamente) al umbral de acusación τ. Operando en la desigualdad, es posible llegar a la siguiente expresión:

$$\begin{aligned}\Pr(NA_l) &= \Pr(M_{BFW} \le \tau) = \Pr\left(\alpha_l / l \le \tau\right) = \Pr(\alpha_l \le \lfloor l\tau \rfloor) \\ \Pr(A_l) &= \Pr(M_{BFW} > \tau) = \Pr\left(\alpha_l / l > \tau\right) = \Pr(\alpha_l > \lfloor l\tau \rfloor) = 1 - \Pr(NA_l)\end{aligned} \tag{7-8}$$

Estas expresiones se corresponden con la función de distribución acumulativa (CDF) de la distribución binomial. La CDF indica la probabilidad de que el valor de una variable aleatoria (α) sea inferior a cierto valor (el valor entero del producto de $|l\tau|$). Es posible entonces derivar las siguientes expresiones de la probabilidad de los estados iniciales A_l y NA_l tras las primeras l observaciones:

$$\begin{aligned}\Pr(NA_l) &= \Pr(\alpha_l \le \lfloor l\tau \rfloor) = \sum_{i=0}^{\lfloor l\tau \rfloor} \binom{l}{i} p_d^i (1-p_d)^{l-i} \\ \Pr(A_l) &= \Pr(\alpha_l > \lfloor l\tau \rfloor) = \sum_{i=\lfloor l\tau \rfloor+1}^{l} \binom{l}{i} p_d^i (1-p_d)^{l-i} = 1 - \Pr(NA_l)\end{aligned} \tag{7-9}$$

Tomando la Figura 7-2 como referencia, el paso siguiente es especificar cual es la probabilidad de transición entre los estados. Dado que hay dos posibles estados, las posibles transiciones son cuatro, aunque en realidad son complementarias dos a dos (la probabilidad de permanecer en un estado o de cambiar al otro han de sumar siempre 1). Cuando un nodo no ha sido acusado, es decir, está en *NA*, puede ocurrir que pase al estado de acusación *A*. En este punto hay que recordar el mecanismo de la métrica BFW. Esta métrica considera únicamente las últimas l observaciones. En otras palabras, cuando hay una nueva observación, descarta la más antigua y recalcula la métrica con el resto de observaciones más la más reciente. Por tanto, para que se dé la circunstancia de una transición del estado de *NA* al de *A* deben cumplirse simultáneamente tres circunstancias: que la observación más antigua fuera una acción cooperativa (con probabilidad 1-p_d), que la observación más reciente sea una acción egoísta (con probabilidad p_d), y además que el número de acciones egoístas en las l-1 observaciones de en medio restantes sea exactamente $|l\tau|$. Si se dan estas condiciones, entonces la observación más reciente de una acción egoísta, hace que la métrica computada en ese momento pase a ser $(|l\tau|+1)/l$ que es mayor que el umbral τ y por tanto desencadena el estado de *A*. Esto puede formularse de la siguiente manera:

$$\Pr(NA \to A) = (1-p_d)p_d \Pr(\alpha_{l-1} = \lfloor l\tau \rfloor) = (1-p_d)p_d \binom{l-1}{\lfloor l\tau \rfloor} p_d^{\lfloor l\tau \rfloor} (1-p_d)^{l-1-\lfloor l\tau \rfloor} \quad (7\text{-}10)$$

$$\Pr(NA \to A) = \binom{l-1}{\lfloor l\tau \rfloor} p_d^{\lfloor l\tau \rfloor + 1} (1-p_d)^{l-\lfloor l\tau \rfloor} \quad (7\text{-}11)$$

Por otro lado, la transición del estado *NA* a permanecer en *NA* sería complementaria:

$$\Pr(NA \to NA) = 1 - \binom{l-1}{\lfloor l\tau \rfloor} p_d^{\lfloor l\tau \rfloor + 1} (1-p_d)^{l-\lfloor l\tau \rfloor} \quad (7\text{-}12)$$

Adicionalmente, las transiciones que parten del estado de acusación son inmediatas, dado que el estado de acusación es absorbente (una vez un nodo retransmisor es acusado, permanece en dicho estado ya que el enlace con dicho nodo se rompe y se trata de establecer otra ruta). Por tanto se podrían formular las siguientes expresiones:

$$\begin{aligned} \Pr(A \to A) &= 1 \\ \Pr(A \to NA) &= 0 \end{aligned} \quad (7\text{-}13)$$

A continuación componemos la matriz *T* de transición de estados:

$$T = \begin{bmatrix} \Pr(NA \to NA) & \Pr(NA \to A) \\ \Pr(A \to NA) & \Pr(A \to A) \end{bmatrix} = \begin{bmatrix} \Pr(NA \to NA) & 1 - \Pr(NA \to NA) \\ 0 & 1 \end{bmatrix} \quad (7\text{-}14)$$

Es posible inferir la siguiente expresión para la potencia *n*-ésima de la matriz *T*:

$$T^n = \begin{bmatrix} \Pr(NA \to NA)^n & 1 - \Pr(NA \to NA)^n \\ 0 & 1 \end{bmatrix} \quad (7\text{-}15)$$

Y finalmente operamos usando las propiedades de las cadenas de Markov para hallar la probabilidad de cada uno de los estados de *A* y *NA* (donde P_0 es el vector de probabilidad de los estados iniciales):

$$P = P_0 T^n = \left(\Pr(NA_l), \Pr(A_l)\right) \times \begin{bmatrix} \Pr(NA \to NA)^{n-l} & 1 - \Pr(NA \to NA)^{n-l} \\ 0 & 1 \end{bmatrix} \quad (7\text{-}16)$$

$$\begin{aligned} \Pr(NA_n) &= \Pr(NA_l) \Pr(NA \to NA)^{n-l} \\ \Pr(A_n) &= 1 - \Pr(NA_l) \Pr(NA \to NA)^{n-l} \end{aligned} \quad (7\text{-}17)$$

Podemos desarrollar estas expresiones para obtener finalmente:

$$\begin{aligned}\Pr(INA) &= F(\lfloor l\tau \rfloor; l, p_d)[(1 - f(\lfloor l\tau \rfloor; l-1, p_d))p_d(1-p_d)]^{n-l} \\ \Pr(IA) &= 1 - F(\lfloor l\tau \rfloor; l, p_e)[(1 - f(\lfloor l\tau \rfloor; l-1, p_e))p_e(1-p_e)]^{n-l}\end{aligned} \tag{7-18}$$

En la expresión 7-18, se ha sustituido el valor de p_d por el de p_e en el caso de *IA*, dado que para que la acusación sea incorrecta, es necesario que p_s=0 y por tanto p_d=p_e. Además, *F* y *f* representan la función de distribución binomial y la función de probabilidad binomial respectivamente:

$$\begin{aligned}f(k; n, p) &= \binom{n}{k} p^k (1-p)^{n-k} \\ F(k; n, p) &= \sum_{i=0}^{k} \binom{n}{i} p^i (1-p)^{n-i}\end{aligned} \tag{7-19}$$

donde *k*, *n* y *p* son los parámetros característicos de la distribución binomial del proceso siguiente: en un experimento que se repite *n* veces, en el que la probabilidad de un suceso es *p* y la de su contrario 1-*p*, cuál es la probabilidad de que el suceso ocurra *k* veces. La Figura 7-3 representa *IA* e *INA* para diferentes probabilidades de egoísmo (p_s) usando las expresiones de 7-18. Se mantiene un valor fijo de *l*=12 y p_e=0.2 y se observa la dependencia de *IA* e *INA* respecto al umbral de acusación τ. Un objetivo de diseño podría ser minimizar *IA* e *INA*, aunque los resultados muestran que ambos siguen tendencias opuestas al variar τ. En las expresiones de *IA* e *INA* (7-18) puede apreciarse que la variación de ambas es opuesta, por el signo – en la ecuación de *IA*. Además, intuitivamente es lógico pensar que un τ bajo fomentará las acusaciones (tanto correctas como incorrectas), mientras que ocurre lo contrario al establecer un τ muy alto, que fomentará que no haya acusaciones. Este compromiso entre *IA* e *INA* se acentúa para un p_s reducido. Si p_s es mayor que 0.3, *INA* es minimizado en τ=0.45, donde *IA* también se anula. Sin embargo, para p_s igual a 0.1 no existe una región donde *IA* e *INA* se anulen.

La Figura 7-4, que representa la variación de *IA* e *INA* respecto al parámetro *l* para valores fijos de τ y p_e, muestra una posible alternativa. *IA* podría reducirse aumentando *l*, pero esto también incrementará *INA* y también el número de paquetes que los nodos egoístas descartarán antes de ser detectados δ. La forma en dientes de sierra de las curvas en la Figura 7-4 se debe a que en las expresiones 7-18 el producto de *l* y τ aparece dentro del operador de parte entera. Debido a que la variación de *IA* e *INA* respecto a *l* no es monótona creciente o decreciente en la Figura 7-4, la optimización del valor de este parámetro es más complicada que en el caso de una variación monótona como la de τ en la Figura 7-3. Sin embargo, se mantiene la tendencia opuesta entre *IA* e *INA*, ya que los picos ascendentes de *IA* coinciden con los picos descendentes de *INA* y viceversa.

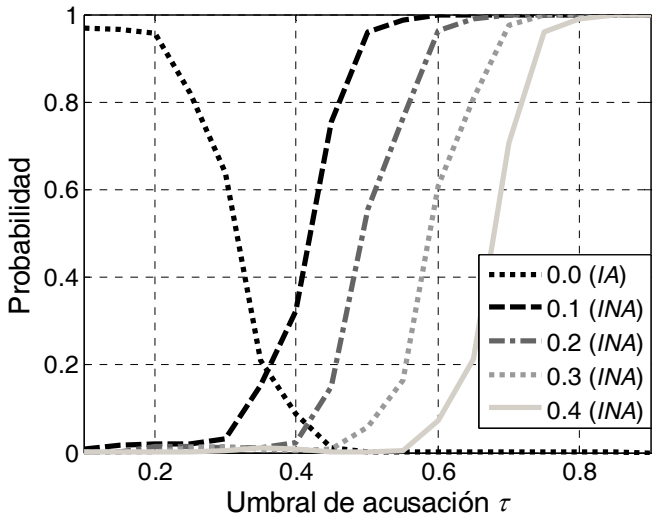


Figura 7-3. *IA* e *INA* en función del umbral de acusación τ. La leyenda corresponde a diferentes valores de p_s.

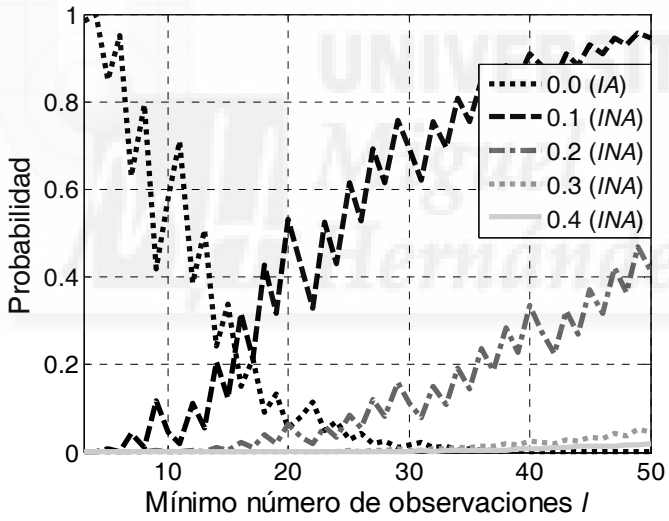


Figura 7-4. *IA* e *INA* en función del mínimo número de observaciones l. La leyenda corresponde a diferentes valores de p_s

Aunque se mantengan fijos los parámetros de configuración l y τ, en la Figura 7-5, p_e también tiene una notable influencia sobre *IA* e *INA*, que vuelven a mostrar tendencias opuestas al variar p_e. Esto quiere decir que l y τ podrían requerir también ser ajustados en función de las condiciones del canal radio. Si la probabilidad del error de observación p_e introducido por el canal es muy alta, esto inducirá a un incremento de las acusaciones, tanto correctas como incorrectas, y viceversa. Este razonamiento intuitivo tiene su reflejo en la Figura 7-5. Distribuciones distintas del parámetro p_s entre los nodos de la red, que son desconocidas a priori, y distintos valores de p_e, requerieren valores distintos de τ y l,

lo cual limita el rendimiento y las posibilidades de implementación del enfoque Bayesiano.

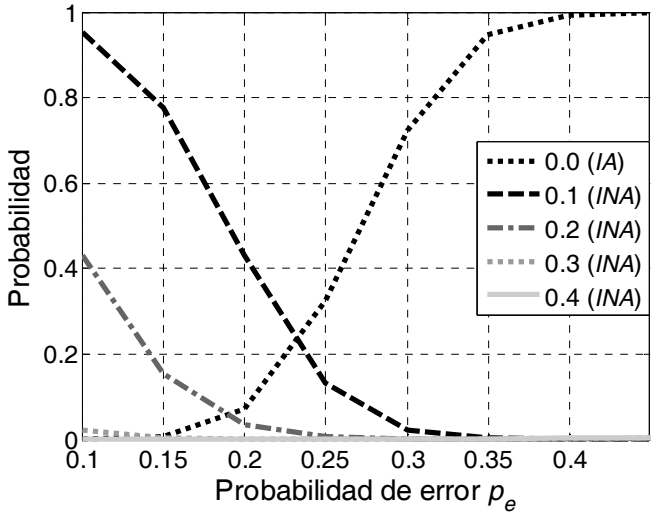


Figura 7-5. *IA* e *INA* en función de la probabilidad de error p_e. La leyenda corresponde a diferentes valores de p_s.

7.2 Técnica de vigilancia exponencial

Para superar las dificultades de las técnicas Bayesianas de detección, se propone un mecanismo exponencial. Esta propuesta define una nueva métrica para comprobar después de cada observación D_n si el número de acciones egoístas observadas α_n tras n observaciones es más probable que se deba al error p_e (provocado por errores en la transmisión radio o colisiones de paquetes), o que se deba al comportamiento egoísta del nodo. Para ello, se necesita una función F_e que mida la probabilidad de la hipótesis H "*H*: *las acciones egoístas observadas se deben a la inexactitud del método de observación exclusivamente"*. Se intentará derivar una función que mida esta probabilidad[36], y que debe cumplir una serie de requisitos:

- F_e debe tener un valor cercano a uno para aquellos valores de α_n que avalen la hipótesis H (y por tanto, p_s=0). Es decir, cuando sea razonable pensar que las acciones egoístas observadas se deben exclusivamente al error de observación p_e y no al egoísmo del nodo.
- F_e debe tener un valor cercano a 0 para los valores de α_n que nieguen la hipótesis H, es decir, cuando sea muy improbable que el número de acciones

[36] Debe aclararse que no se busca una función que mida exactamente la probabilidad de la hipótesis expresada, sino más bien una función aproximada sencilla que tenga el comportamiento expresado en los requisitos.

egoístas observadas se deban únicamente al error de observación de la técnica, sino que son consecuencia tanto de ese error como del egoísmo del nodo p_s>0.

- F_e debe tener un valor intermedio, no próximo a 0 ni a 1, cuando a partir del número de acciones egoístas observadas no sea posible determinar con precisión si el nodo se comporta de manera egoísta. En esta zona debe ser monótona. creciente. La Tabla 7-1 resume estos requisitos:

Valor esperable de p_s	Valor de F_e
$p_s = 0$	$F_e \sim 1$
$p_s > 0$	$F_e \sim 0$
p_s ?	$0 < F_e < 1$

Tabla 7-1. Requisitos de la función F_e.

Para encontrar la función F_e, se parte en primer lugar de las expresiones en la ecuación 7-19 que representan la función de distribución binomial $F(k;n,p)$ y la función de probabilidad binomial $f(k;n,p)$. La función de distribución binomial $F(k;n,p)$ calcula la probabilidad de que al repetir un experimento aleatorio con dos posibles salidas (éxito o fracaso), con probabilidad de éxito p, al cabo de n experimentos el número de éxitos total sea igual o menor que k. La función de probabilidad binomial $f(k;n,p)$ calcula la probabilidad de que el número de éxitos sea igual a k, en las mismas condiciones. En la técnica de *watchdog*, el parámetro k se corresponde con el número de acciones egoístas observadas α_n, el parámetro n coincide en ambas, y el parámetro p se corresponde con la probabilidad de detectar una acción egoísta p_d. Recuérdese que p_d incluía los efectos combinados del error de *watchdog* p_e y la probabilidad de egoísmo del nodo p_s (ecuación 7-1). Supóngase que se dispone de alguna técnica para obtener una estimación de la probabilidad de error en la observación de la retransmisión de los paquetes p_e. Supóngase también en principio que p_s=0, es decir, suponemos que el nodo que estamos observando no es egoísta (lo cual concuerda con la hipótesis establecida H). En este caso, $f(\alpha_n;n,p_e)$ calcularía la probabilidad de que tras n observaciones el número de acciones egoístas observadas fuera exactamente α_n. $F(\alpha_n;n,p_e)$ calcularía la probabilidad de que el número de acciones egoístas observadas fuera igual o menor a α_n. Sin embargo, estas funciones no cumplen los requisitos que se habían marcado para la función F_e, lo cual puede apreciarse en la Figura 7-6 donde se representan ambas a modo de ejemplo. Los valores de los parámetros utilizados son n=30, p=0.4 y k variando entre 0 y n. En estas condiciones, el valor más probable de la variable α_n es α_n=12=$n \cdot p_e$. Si tras n=30 observaciones obtenemos que α_n=12, deberíamos concluir que la hipótesis es cierta, ya que es bastante probable que esas acciones egoístas se deban al error de observación p_e que hemos estimado y no al egoísmo del nodo. Sin embargo, en ese punto las funciones

de probabilidad $F(\alpha_n;n,p_e)$ y $f(\alpha_n;n,p_e)$ dan valores bajos, cuando la función buscada debería dar un valor cercano a 1 (según la Tabla 7-1). Además, la función $F(\alpha_n;n,p_e)$ tampoco se ajusta al requisito de que la función buscada $F_e \sim 0$ debe ser cercana a 0 cuando sea muy improbable que el número de acciones egoístas observadas α_n se deban únicamente al error de observación de la técnica. Por ejemplo, es muy improbable que un número de acciones egoístas elevado como α_n=25 se deba exclusivamente al error estimado de p_e=0.4, lo cual induce a sospechar que no se cumple la hipótesis y que p_s>0. En estas condiciones, debería cumplirse $F_e \sim 0$ mientras que $F(25;30,0.4) \sim 1$. Por todo esto se descartan ambas funciones y se hace necesario buscar alternativas.

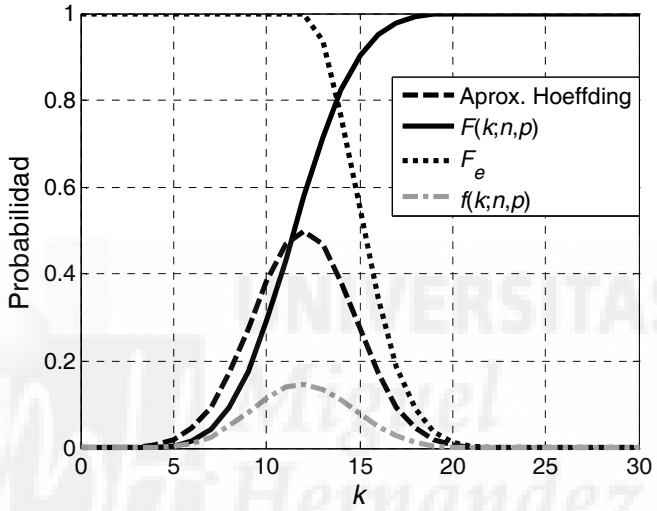


Figura 7-6. Función de distribución Binomial $F(k;n,p)$, aproximación basada en la desigualdad de Hoeffding y función exponencial propuesta F_e

En la Figura 7-6 se representa una función alternativa, que es una aproximación a la función de distribución $F(k;n,p)$. Dicha aproximación expresa una cota superior de $F(k;n,p)$ para valores de $k \leq n \cdot p$ (ecuación 7-20).

$$F(k;n,p) \leq \frac{1}{2}\exp\left(-2\frac{(np-k)^2}{n}\right) \tag{7-20}$$

donde los parámetros k, n y p son los característicos de la distribución Binomial como en la expresión 7-19. Se aprecia en la Figura 7-6 que efectivamente la aproximación es una cota superior de F útil exclusivamente para los valores especificados $k \leq n \cdot p$; aunque por otro lado tampoco cumple con los requisitos establecidos anteriormente para la función F_e. Sin embargo, puede tomarse como referencia esta función y modificarla para ajustarla a los requisitos. Para ello se realizan las siguientes modificaciones *ad hoc*:

- Para elevar el valor máximo de la función a 1, se elimina el factor multiplicativo ½.
- Para hacer que el valor de la función sea 1 cuando se cumple $k \leq n \cdot p$ (región en la que es justificado pensar que las acciones egoístas observadas se deben exclusivamente al error de *watchdog*), se utiliza el operador $\Delta\_$ expresado en la ecuación 7-21. Dicho operador tiene la propiedad de que, para los valores positivos de x se anula, mientras que para los valores negativos de x es la función identidad. Este comportamiento es el buscado porque $e^0=1$, que es el valor deseado de la función F_e en la región $k \leq n \cdot p$, expresado de manera equivalente $\alpha_n \leq n \cdot p_e \rightarrow n \cdot p_e - \alpha_n \geq 0$, siendo $n \cdot p_e - \alpha_n$ la expresión que aparece dentro de la función exponencial en la ecuación 7-20. Por tanto, en la región de interés $\alpha_n \leq n \cdot p_e$, el operando de la función exponencial se anularía al introducir el operador $\Delta\_$, y F_e tendría valor unidad.

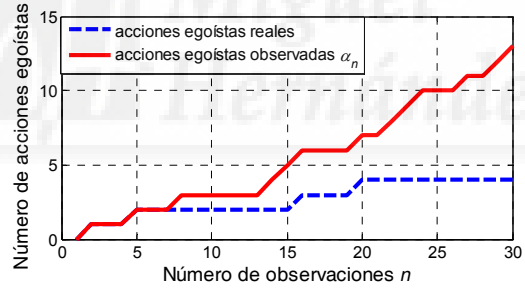
$$\Delta\_(x) = \frac{x - |x|}{2} = \begin{cases} 0 & x \geq 0 \\ x & x < 0 \end{cases} \tag{7-21}$$

Con estas indicaciones, se propone la función F_e (ecuación 7-22) que cumple los requisitos de diseño marcados, tal como se aprecia al representarla en la Figura 7-6. Puede apreciarse en la Figura 7-6 que, al tomar un valor del parámetro k reducido (y por tanto, un número reducido de acciones egoístas detectadas), lo más probable es que las acciones egoístas se deban al error de la técnica de observación y por tanto F_e vale 1 (se cumple la hipótesis H). Sin embargo, conforme el valor de k crece y se cumple $k > p \cdot n$, entonces la probabilidad de las acciones egoístas detectadas se deban exclusivamente al error de la técnica disminuye progresivamente, como refleja la Figura 7-6, hasta ser casi nulo en los valores más altos de k.

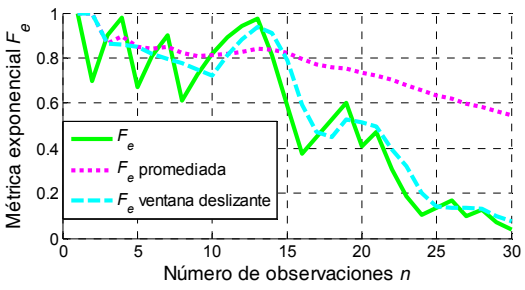
$$F_e(\alpha; n, p_e) = \exp\left(-2 \frac{(\Delta\_(np_e - \alpha_n))^2}{n} \right) \tag{7-22}$$

La función F_e cumple los requisitos buscados y podría por tanto ser empleada como métrica para evaluar si los nodos se están comportando egoístamente. El proceso sería el siguiente: tras cada observación de una retransmisión, o de una acción egoísta, se evalúa la función F_e y se comprueba si su valor es superior a un cierto valor umbral τ. En caso de que sea así, se da por válida la hipótesis H de que las acciones egoístas observadas son debidas al error de *watchdog*. De lo contrario, se acepta lo contrario, es decir, el nodo que está siendo vigilado está llevando a cabo acciones egoístas por encima del error estimado de *watchdog*. Sin embargo, es posible comprobar que al emplear directamente la función F_e para el proceso de detección, los valores obtenidos tienden a sufrir oscilaciones que

podrían afectar negativamente al proceso de detección. Para comprobarlo, se ha representado en la Figura 7-7 una muestra aleatoria del proceso de observación de retransmisiones (Figura 7-7(a)) y la evaluación de la métrica exponencial F_e para esa muestra en tiempo real (Figura 7-7(b)), para la cual además se han realizado distintos promedios. Se trata de una muestra aleatoria con un número de observaciones total de 30, en la que la probabilidad de error del *watchdog* se establece en p_e=0.2 y la probabilidad de egoísmo del nodo en p_s=0.2. El proceso se representa con dos parámetros en la Figura 7-7(a): el número de acciones egoístas reales llevadas a cabo por el nodo retransmisor y el número de acciones egoístas observadas α_n por el nodo precursor. Por otro lado, en la Figura 7-7(b) se representa el valor de la función propuesta F_e tras cada observación realizada. Cuando la función F_e desciende de un cierto umbral τ, el nodo debería ser acusado. Sin embargo, pueden apreciarse las oscilaciones bruscas que aparecen en la curva de F_e, que podrían hacer que hubiera algún descenso puntual que provocara la acusación de un nodo que en realidad fuera cooperativo. Para evitarlo, se propone promediar la función F_e con dos alternativas: o bien promediar todos los valores de F_e tras cada observación (F_e promediada) o bien tomar sólo los últimos valores de F_e cada vez (F_e ventana deslizante). En ambos casos se consiguen evitar las oscilaciones bruscas de F_e, tanto más cuanto más valores se toman para hacer el promedio. El tamaño de ventana ha sido de 3 muestras.



(a)



(b)

Figura 7-7. Muestra aleatoria del proceso de observación de retransmisiones (a) y representación de la función métrica exponencial F_e con distintos promedios (b).

Considerando la discusión anterior, se propone la siguiente métrica para el proceso de detección exponencial. Después de cada observación, se calcula la función exponencial (7-22) a partir de los datos registrados y de la nueva observación, y se almacena su salida en un registro. A continuación se proponen dos métricas con distinto tamaño de promediado. La primera, EIW (*Exponential Infinite Window*), se define como el promedio de todas las salidas almacenadas (contando a partir del mínimo de observaciones *l*). Por otro lado, la métrica alternativa EFW (*Exponential Finite Window*) considera sólo las últimas *l* salidas, donde *l* sigue siendo también el mínimo número de observaciones necesario para asegurar la fiabilidad del resultado:

$$M_{EIW}(n,\alpha,l)=\frac{1}{l}\sum_{i=l}^{n}\exp\left(-2\frac{\left(\Delta_{-}(ip_e-\alpha_i)\right)^2}{i}\right)\Bigg|_{n\geq l}$$
$$M_{EFW}(n,\alpha,l)=\frac{1}{l}\sum_{i=n-l+1}^{n}\exp\left(-2\frac{\left(\Delta_{-}(ip_e-\alpha_i)\right)^2}{i}\right)\Bigg|_{n\geq l} \quad (7\text{-}23)$$

A diferencia del enfoque Bayesiano, la propuesta exponencial acusa a un nodo de actuar egoístamente cuando el valor de la métrica es inferior al umbral de acusación τ. En este caso debe señalarse que τ no está directamente relacionado con la distribución de nodos egoístas $f_{ps}(x)$ y con el error p_e introducido por la técnica de observación, sino que se puede variar para facilitar el ajuste de las tasas de error *IA* e *INA*. Esto contribuye a la selección de un valor adecuado de τ y mejora las perspectivas de implementación de la propuesta exponencial respecto a las técnicas Bayesianas, como se muestra en las Figuras 7-8(a) y 7-8(b). Las líneas continuas representan la CDF del número de acciones egoístas observadas α para diferentes valores de p_s. α representa los paquetes que el nodo precursor observa como "no retransmitidos", bien por el error de la técnica de observación p_e o por el egoísmo del nodo p_s. La CDF muestra la probabilidad de que α sea menor a cierto valor *x*, considerando p_s={0,0.1,0.3} y p_e=0.1 en la Figura 7-8(a) y p_e=0.2 en la Figura 7-8(b). Las CDFs se obtienen de la función de distribución Binomial (ecuación 7.19) para $p=p_d$ en la ecuación 7.1. Las líneas de puntos representan la métrica Bayesiana (α/n) y la expresión de la función F_e (7-22) usada en la métrica exponencial (7-23). Supóngase un límite de acusación α_0 de 13 en la Figura 7-8(a) y de 23 en la Figura 7-8(b); el límite de acusación representa el máximo número de paquetes observados como no retransmitidos antes de que se realice la acusación. En la Figura 7-8(b), un valor estimado de p_e mayor requiere incrementar el límite de acusación α_0 dado que habrá un mayor número de observaciones incorrectas (que, de mantenerse un α_0 bajo, llevarían a acusaciones incorrectas). En este caso, los límites de acusación se han escogido como un compromiso entre la *IA* de los nodos cooperativos y la *INA* de los nodos con egoísmo p_s=0.1 e implican diferentes valores del umbral de acusación τ para cada métrica (τ_{bay} y τ_{exp} en las figuras). De hecho, los límites de acusación determinan dos zonas diferentes en

el eje *x*: una zona de no acusación para los valores de $\alpha < \alpha_0$, y una zona de acusación para los valores superiores de $\alpha > \alpha_0$. Cuando α alcance o supere α_0, la métrica debería ser tal que indicara que el nodo debe ser acusado, es decir, debe ser igual al umbral de acusación. Según este razonamiento, los respectivos umbrales de acusación de cada métrica τ_{bay} y τ_{exp} pueden obtenerse como la intersección entre el límite de acusación (determinado por $\alpha = \alpha_0$) y la curva de la métrica correspondiente. Dichos puntos de interesección han sido marcados en las Figuras 7-8(a) y 7-8(b). Por otro lado, también es posible recabar información en las figuras sobre las tasas de error *IA* e *INA* y su relación con los umbrales de acusación. Recuérdese que la CDF describe la probabilidad *p* de que el número de acciones egoístas observadas sea igual o inferior a cierto valor de α. Igualmente se puede obtener la probabilidad de que el número de acciones egoístas sea superior a cierto valor de α, haciendo la operación complementaria 1-*p*. Tomando como valor de α el límite de acusación α_0 en la CDF de los nodos cooperativos (p_s=0), obtenemos la probabilidad *p* de que no se realice una acusación a un nodo cooperativo. El complementario 1-*p* es justamente la tasa de error *IA* (acusaciones a nodos cooperativos). Gráficamente, en la Figura 7-8, este valor es el segmento determinado por el punto de intersección entre la CDF de los nodos cooperativos y el límite de acusación $\alpha = \alpha_0$, y el punto en la gráfica $(\alpha_0 , 1)$. Analíticamente:

$$IA = 1 - F(\alpha_0; n, p_e) \tag{7-24}$$

Análogamente, *INA* es la probabilidad de que los nodos egoístas no sean acusados. En este caso, dado que $p_d = p_s + p_e + p_s \cdot p_e$, *INA* depende no solamente de p_e sino que será diferente para cada p_s. En la Figura 7-8 se ha considerado únicamente p_s=0.1, que por otro lado es el que obtiene un valor más alto de *INA*. Por el mismo procedimiento anterior, *INA* está determinada por la intersección entre el límite de acusación α_0 y la CDF de los nodos egoístas con p_s=0.1. Dicho punto de interesección representa la probabilidad de que el número de acciones egoístas detectadas α sea igual o menor que el límite de acusación α_0 establecido. Es posible derivar la expresión:

$$INA = F(\alpha_0; n, p_d) \tag{7-25}$$

Es importante señalar que en el caso de la función exponencial, τ_{exp} se mantiene aproximadamente constante para p_e=0.1 y p_e=0.2 en las Figuras 7-7(a) y 7-7(b). Esto se debe a que p_e se considera explícitamente en la función exponencial de forma que la curva de su métrica se desplaza cuando cambia p_e. Por el contrario, τ_{bay} debe ser reajustado cuando cambia p_e en la Figura 7-7(b), lo cual subraya la necesidad de ajustar el valor óptimo de τ_{bay} para cada p_e. Otra importante diferencia entre ambos enfoques es que en el exponencial la métrica consiste en el promedio de las últimas *l* salidas y no únicamente la última, amortiguando el efecto de observaciones incorrectas temporales.

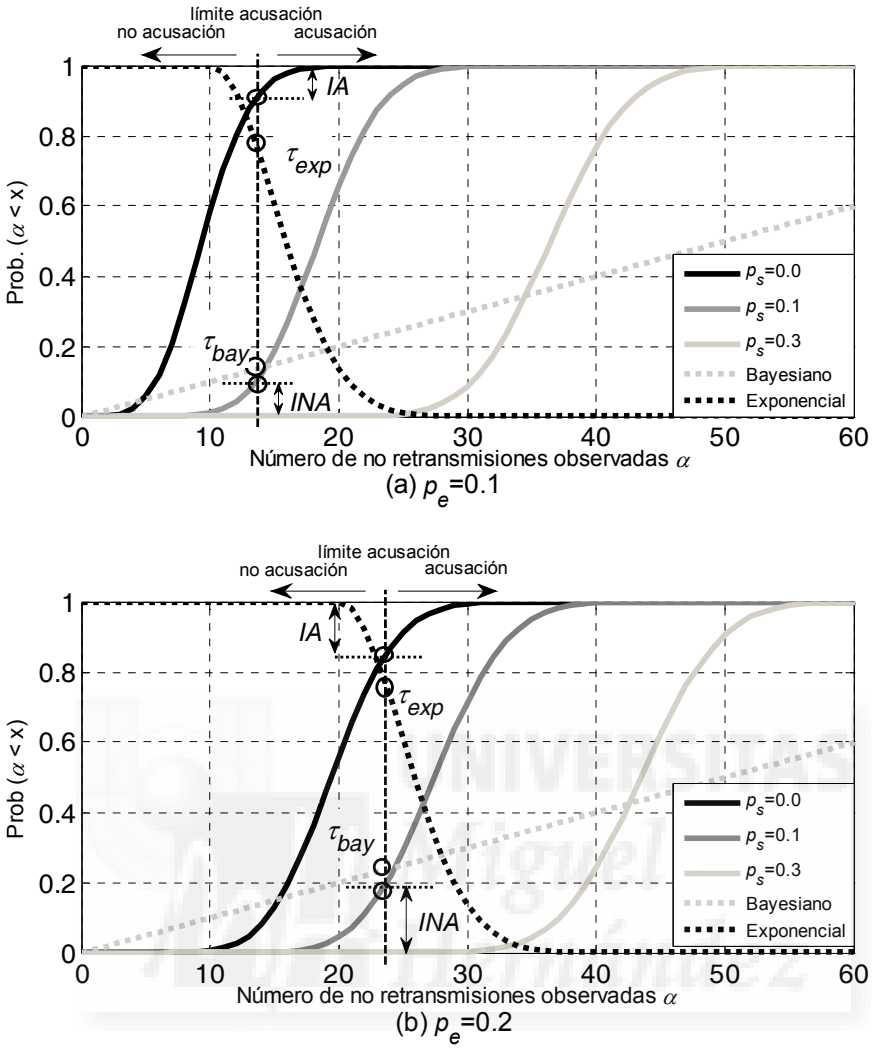


Figura 7-8. Representación y parámetros de las funciones exponencial y Bayesiana.

7.3 Evaluación experimental

7.3.1 Métricas de evaluación

En este apartado se evalúa experimentalmente el rendimiento de todas las métricas presentadas en el capítulo, tanto la métrica Bayesiana y sus variantes como las dos variantes de la métrica exponencial propuesta. El objetivo es mostrar comparativamente su rendimiento, tanto en términos de precisión como de velocidad, y su robustez frente a la variación de diferentes parámetros como el número de observaciones N y la probabilidad de error p_e.

Los parámetros de rendimiento que serán evaluados son la tasa de acusaciones incorrectas *IA* y la tasa de no acusaciones incorrectas *INA*, en cuanto a la precisión, y el

número de paquetes descartados por nodos egoístas antes de ser detectados δ, en cuanto a la velocidad. Recuérdese que *IA* se calcula como el cociente entre el número de nodos cooperativos acusados y el número total de nodos cooperativos en la red y es una medida de la capacidad de la técnica para evitar acusaciones incorrectas a nodos cooperativos. Por otro lado, *INA* se define como el cociente entre el número de nodos egoístas no acusados y el número total de nodos egoístas. Es por tanto una medida de la sensibilidad de la métrica para detectar los nodos egoístas: cuanto menor es su valor, más sensible es a los nodos egoístas (más probable es que los detecte). *INA* depende del parámetro de egoísmo p_s de cada nodo, es decir, la sensibilidad de las métricas es diferente para cada tipo de nodo. Un nodo con una p_s muy alta es más fácil de detectar que un nodo con una p_s baja, cuyo comportamiento egoísta puede ser enmascarado por el error de observación. Por tanto, en general la *INA* de los nodos menos egoístas es mayor. Por otro lado, tanto *IA* como *INA* también dependen de la probabilidad de error p_e. A mayor p_e, mayor incertidumbre habrá en el proceso de detección y por tanto será más inexacto, aumentando tanto *IA* como *INA*. Todo esto puede apreciarse tanto en la Figura 7-8 como en las expresiones 7-24 y 7-25. Cabe recordar por último que *IA* e *INA* siguen tendencias opuestas frente a los parámetros de configuración τ y l, tal y como reflejan las Figuras 7-3 y 7-4, lo cual hace necesario un proceso de selección del valor óptimo de estos parámetros como se explicará más adelante.

Por otro lado, el parámetro δ mide la capacidad de detectar con rapidez a los nodos egoístas. Es preferible un δ reducido, ya que cuanto menor es δ, menos paquetes descartan los nodos egoístas antes de ser detectados. δ, al igual que *INA*, se ve afectado también por el parámetro p_s. Cuanto mayor es el egoísmo (mayor es p_s), más rápidamente son detectados los nodos, y por tanto, a pesar de que descartan una proporción mayor de paquetes, son detectados antes y el δ resultante es menor. Este parámetro también deberá ser tenido en cuenta a la hora de configurar la pareja de parámetros (τ,l).

7.3.2 Escenarios de evaluación

Se han llevado a cabo simulaciones de las técnicas exponenciales y Bayesianas en escenarios con diferentes parámetros de entrada p_s, p_e y N. Los parámetros de rendimiento son sensibles a la variación de p_s, y por tanto es necesario considerar diferentes valores. p_s variará de 0 (nodos cooperativos) a 1.0 (nodos siempre egoístas), en escalones de 0.1. Aunque en una red real p_s podría tomar cualquier valor entre 0 y 1, este conjunto de valores es suficiente para la evaluación. Por otro lado, p_e toma los valores del conjunto {0.1,0.2,0.3,0.4}. Hay que señalar que en una situación real p_e puede ser mayor que 0.4. Sin embargo, resulta más razonable utilizar la técnica de *watchdog* cuando la p_e se encuentre dentro de este rango, ya que de otro modo la incertidumbre del proceso

puede ser muy alta[37]. El parámetro N toma valores en el conjunto $\{50,75,100,200,300,400,500\}$. N representa el número total de observaciones que se han podido realizar antes de que el enlace haya caído, o la comunicación haya finalizado por no existir más datos que transmitir (no confundir con el número de simulaciones realizadas). N depende de los factores que pueden afectar a la duración del enlace, como la movilidad y el tipo de canal del escenario, o al número de paquetes enviados por unidad de tiempo, como la velocidad de generación y transmisión de los datos. El rango de valores escogido da una idea de la influencia de N en distintas situaciones: alta movilidad y presencia de obstáculos en el canal de propagación (que resultan en enlaces de breve duración y pocos paquetes transmitidos) o en escenarios más estables (donde el número de paquetes transmitidos puede ser mucho mayor).

Parámetro	Error relativo máximo [%]
IA	0.51
INA	0.38
δ	0.16

Tabla 7-2. Error relativo máximo [%].

En cuanto al método de evaluación, se han realizado experimentos iterativos basados en el proceso de detección explicado en el apartado 7.1. El número total de experimentos (15000) garantiza que los resultados obtenidos tienen un error relativo menor al 0.51%, tal y como muestra la Tabla 7-2. En cada experimento, se extrae y evalúa una secuencia de muestra $\{a_n\}$ de N observaciones. Cada muestra a_n consiste en un vector de N elementos, cada uno de los cuales puede ser o 1 o 0, representando respectivamente la observación de una acción egoísta o de una acción cooperativa. El proceso de observación es independiente de la métrica, y por tanto en cada iteración, la misma muestra a_n es evaluada por los 6 mecanismos de detección m presentados en el apartado 7-2. Cada mecanismo m indica que el nodo está actuando egoístamente según si su métrica da un resultado positivo en alguna de las observaciones α_n de la muestra, donde n debe estar entre $l \le n \le N$. Si no resulta acusado en ninguna $n \le N$, entonces resulta una no acusación. Una acusación es incorrecta si $p_s=0$ para esa muestra, y una no acusación es incorrecta si $p_s>0$. Para la obtención del valor de las métricas de resultados antes mencionadas, se obtienen los promedios de los parámetros *IA*, *INA* y δ para todas las iteraciones realizadas, bajo distintos parámetros de entrada. Sea $x_i \in \{0.0,0.1,...,1.0\}$ con

[37] En la Figura A-II-9 del anexo A-II se muestran los valores de p_e obtenidos en promedio en lotes de simulaciones realizadas con la plataforma de simulación descrita en el capítulo 4, y ampliada para cubrir algunos aspectos de redes multi-salto celulares, tal como se explica en el capítulo 8 y en el anexo A-I. Puede observarse en la Figura A-II-9 que el número de ocasiones en que $p_e > 0.5$ es significativo.

$i = 1,..., N_{ps}$, N_{ps}=11, el conjunto de los posibles valores discretos del parámetro p_s con función de probabilidad $f_{ps}(x)$ en un conjunto de nodos. N_{ps} representa el número de niveles discretos de p_s (por simplicidad, se considera p_s como una variable aleatoria discreta). Los valores promedios de *IA*, *INA* y δ, pueden calcularse usando el principio de proporcionalidad expresado en las siguientes ecuaciones:

$$\begin{aligned} \overline{IA}(m, f_{ps}, \tau, l, N, p_e) &= f_{ps}(0.0) IA(m, \tau, l, N, p_e) \\ \overline{INA}(m, f_{ps}, \tau, l, N, p_e) &= \sum_{i=2}^{N_{ps}} f_{ps}(x_i) INA(m, x_i, \tau, l, N, p_e) \\ \overline{\delta}(m, f_{ps}, \tau, l, N, p_e) &= \sum_{i=2}^{N_{ps}} f_{ps}(x_i) \delta(m, x_i, \tau, l, N, p_e) \end{aligned} \tag{7-26}$$

En el apartado 7.1.2 se mostró que los parámetros de configuración τ y l influyen notablemente en el rendimiento de las técnicas. *IA*, *INA* y δ siguen tendencias opuestas frente a la variación de τ y de l como mostraban las Figuras 7-3 a 7-5. Por tanto, τ y l deben configurarse adecuadamente para cada técnica, teniendo en cuenta las variaciones en todos los parámetros de entrada (m,p_s,N,p_e). Para ello, la selección de los valores óptimos de τ y l será llevada a cabo en escenarios[38] que reflejen un equilibrio entre la importancia de *IA*, *INA* y δ. Por esta razón, se define un conjunto de distribuciones $f_{ps}^{i}(x)$ que reúnen dos factores con un importante impacto en *IA* e *INA*: la proporción de nodos no egoístas $f_{ps}(0)$ y la proporción de nodos con un egoísmo p_s reducido pero no nulo $f_{ps}(0.1)$. La proporción de nodos no egoístas $f_{ps}(0)$ influye principalmente en el promedio de *IA*, como muestra la ecuación 7-26, mientras que la proporción de nodos con p_s=0.1 guarda relación con el promedio de *INA* (ya que los nodos con un p_s próximo a 1 suelen ser fácilmente detectables y por tanto *INA* tiende a ser nula). Intuitivamente, si en un conjunto de nodos son más numerosos los nodos cooperativos, es importante escoger los parámetros τ y l de manera que la *IA* sea lo más reducida posible, aún a costa de aumentar ligeramente la *INA*. A la inversa, si la proporción de nodos con un egoísmo reducido pero no nulo $f_{ps}(0.1)$ es mayor, entonces es más prioritario reducir la *INA*. El equilibrio entre ambas tendencias se alcanza considerando en las simulaciones 24 combinaciones diferentes de 8 proporciones de nodos no egoístas ($f_{ps}(0) \in \{0.1,0.2,...,0.8\}$), y 3 formas de función (uniforme, linealmente creciente y decreciente) para la $f_{ps}(x)$ de los nodos egoístas: una función decreciente representa una red con un número más grande de nodos con p_s=0.1. La Figura 7-9 representa alguna de estas funciones. En la fila superior (Figuras 7-9(a), 7-9(b), 7-9(c)) se representan tres $f_{ps}(x)$ con $f_{ps}(0)$=0.2 mientras en la fila

[38] Por escenario nos referimos a una determinada distribución del egoísmo de los nodos en una red $f_{ps}(x)$.

inferior (Figuras 7-9(d), 7-9(e), 7-9(f)) se muestran tres distribuciones $f_{ps}(x)$ con $f_{ps}(0)$=0.8.

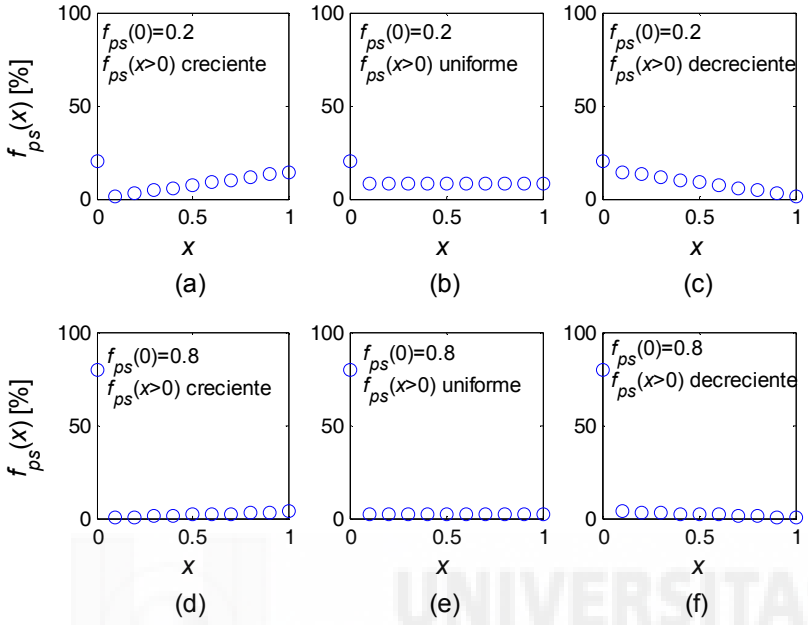


Figura 7-9. Distintas distribuciones de probabilidad del parámetro p_s

7.3.3 Velocidad y precisión de detección

IA, *INA* y δ se promedian en el conjunto de distribuciones $\{f_{ps}^{i}(x)\}_{i=1}^{24}$ considerado y en el número máximo de observaciones antes de la finalización del enlace *N*. El criterio para seleccionar el (τ,*l*) óptimo para cada métrica *m* y para cada p_e es minimizar la suma de los parámetros *IA*, *INA* y δ para obtener la mejor combinación de velocidad y precisión. El conjunto de valores de (τ,*l*) evaluados incluye todas las combinaciones de los valores $\tau \in \{0.1,0.15,\ldots,0.9\}$ y $l \in \{3,6,12,24,48\}$. Los valores (τ,*l*) seleccionados finalmente a través de esta metodología se muestran en las Tablas 7-3 y 7-4. Todas las técnicas Bayesianas deben reajustar el valor de τ para cada valor de p_e, dado que debe cumplirse $\tau > p_e$ para que no aumente *IA*, pero a su vez τ no debe ser tan grande como para que los nodos con reducido p_s no sean detectados. Por contra, EFW no necesita ajustar τ porque se descuenta en la función exponencial (ecuación 7-22). Debe señalarse que tanto las técnicas Bayesianas como las exponenciales deben estimar el valor de p_e, bien para ajustar el parámetro τ en el primer caso, o para calcular correctamente la función exponencial en la expresión 7-21 en el segundo caso. Por tanto, la estimación de p_e no es una desventaja de las técnicas exponenciales.

p_e	BIW	BFW	BDF	BFWDF	EIW	EFW
0.1	0.30	0.45	0.40	0.45	0.40	0.10
0.2	0.40	0.45	0.50	0.40	0.35	0.10
0.3	0.45	0.55	0.50	0.65	0.35	0.10
0.4	0.55	0.60	0.50	0.65	0.35	0.10

Tabla 7-3. Valores de τ para rendimiento promedio optimizado.

p_e	BIW	BFW	BDF	BFWDF	EIW	EFW
0.1	12	12	48	12	3	3
0.2	12	24	6	48	6	3
0.3	24	24	12	12	6	3
0.4	24	48	48	24	6	3

Tabla 7-4. Valores de l para rendimiento promedio optimizado.

Las Figuras 7-10, 7-11 y 7-12 muestran la influencia de N en los parámetros *IA*, *INA* y δ. Los valores seleccionados para los valores de configuración τ y l son los mostrados en las Tablas 7-3 y 7-4, con los cuales se obtiene el mejor rendimiento en promedio (para los valores de p_e considerados). La técnica EFW mejora la precisión de la detección, al reducir el número de nodos egoístas que no son acusados (tasa de error *INA*). Esto quiere decir que la sensibilidad a los nodos egoístas es mayor que en el resto de las técnicas. Este aumento de la precisión se consigue sin incurrir en un alto número de paquetes descartados en la Figura 7-12 para las dos técnicas exponenciales. Esto se debe a que los valores del parámetro l (seleccionados a través del proceso de optimización) para las técnicas exponenciales son menores que para las técnicas Bayesianas en las Tablas 7-3 y 7-4. Las técnicas Bayesianas necesitan un mayor número mínimo de observaciones l para determinar con precisión si un nodo es egoísta. Por el contrario, las técnicas exponenciales pueden tomar las decisiones de acusación o no acusación tras haber realizado un número menor de observaciones, sin por ello incurrir en un aumento de las acusaciones incorrectas (*IA*, Figura 7-10). La Figura 7-10 muestra que hay dos técnicas Bayesianas (BFW y BFWDF) que obtienen una menor *IA* para valores reducidos de N, pero esto es a cambio de una gran imprecisión en *INA*. Se observan dos efectos cuando se incrementa N: los nodos egoístas son más fáciles de detectar (Figura 7-11), pero por otro lado se incrementa el número de descartes δ (Figura 7-12). Ambos efectos están relacionados. Al incrementar N, las técnicas disponen de mayor información para determinar si un nodo es egoísta. Esto es aplicable sobre todo a los nodos con un egoísmo menor (con un valor reducido de p_s). Cuando el egoísmo del nodo es muy elevado,

incluso con pocas observaciones se puede asegurar que un nodo se está comportando egoístamente. En cambio, cuando p_s es bajo, entonces para que sean detectados es deseable tener un número mayor de observaciones, es decir, valores altos de N. Del mismo modo, los nodos con egoísmo reducido que con valores bajos de N no eran detectados y con valores altos de N sí, hacen que se incremente el número de descartes δ, debido a que cuando son detectados han tenido tiempo ya de descartar algunos paquetes. Sin embargo, dado que precisamente estos nodos son los que menos paquetes descartan, el incremento en δ que puede apreciarse en la Figura 7-12 al aumentar N no es muy acusado, pero sí generalizado para todas las técnicas.

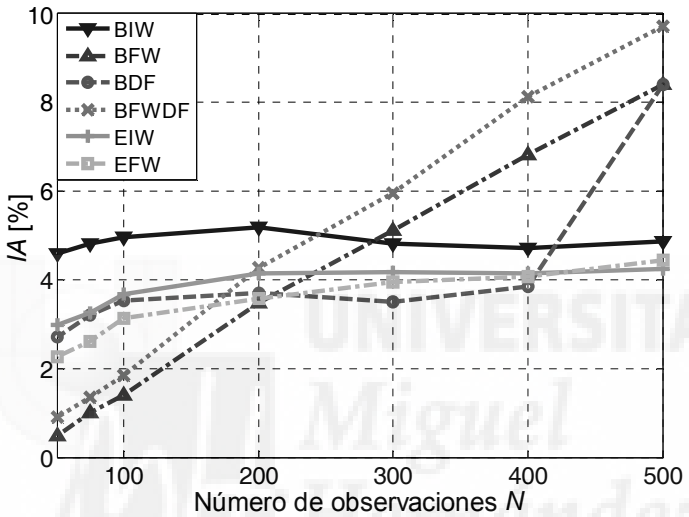


Figura 7-10. Tasa de acusaciones incorrectas en función del número máximo de observaciones.

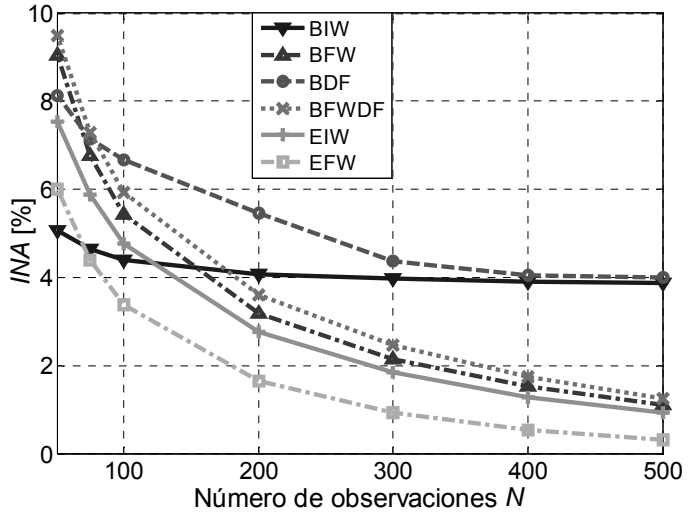


Figura 7-11. Tasa de no acusaciones incorrectas en función del número máximo de observaciones.

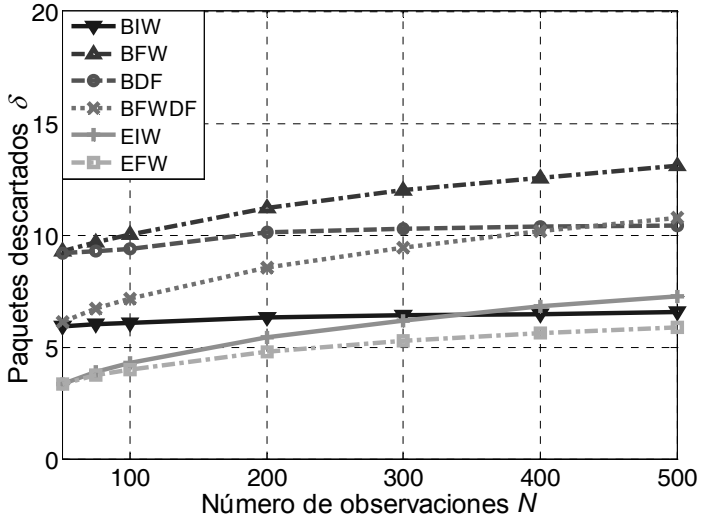


Figura 7-12. Número de paquetes descartados por egoístas antes de su detección en función del número máximo de observaciones

El valor de p_e condiciona la selección de los valores (τ,l) para las técnicas Bayesianas (Tablas 7-3 y 7-4), e influye por tanto también en la precisión y la velocidad de los mecanismos de detección (Figuras 7-13, 7-14 y 7-15). Las Figuras 7-13, 7-14 y 7-15 muestran el efecto de p_e en la precisión de la detección (*IA* e *INA*) y en la velocidad (δ). En primer lugar, es necesario aclarar que la variación no uniforme de los parámetros de rendimiento *IA*, *INA* y δ en función de p_e de las técnicas Bayesianas se explica por el ajuste de los parámetros de detección al variar p_e. Dicho ajuste se llevó a cabo mediante el procedimiento descrito al principio de esta sección 7.3.3, y del que se obtuvieron los valores expresados en las Tablas 7-3 y 7-4. Se demostró que las técnicas Bayesianas deben reajustar el valor de τ para cada valor de p_e, para que siempre se cumpla que $\tau > p_e$. En caso de que τ fuera menor que p_e, entonces el número de acusaciones incorrectas aumentaría debido a que se producirían errores de observación que en realidad serían atribuibles al egoísmo del nodo. De hecho, τ debe ser igual a p_e más un cierto margen, el cual no debe ser tan grande como para que los nodos con reducido p_s no sean detectados. La elección del valor de τ es por tanto un compromiso entre las tasas de *IA* e *INA*. El hecho de tener que reajustar cada vez τ hace que también se tenga que ajustar el valor de l, ya que ambos influyen conjuntamente en los tres parámetros utilizados para la selección de los valores óptimos de l y τ: *IA*, *INA* y δ. Por contra, en las técnicas exponenciales no es necesario el reajuste en el valor de τ al variar la p_e, ya que el valor de p_e ya está descontado en la función exponencial (ecuación 7-22), y por ello la variación de los parámetros *IA*, *INA* y δ frente a p_e es más uniforme en las Figuras 7-13, 7-14 y 7-15. En dichas figuras puede apreciarse que el incremento del error de observación p_e perjudica en general tanto a la precisión como a la velocidad de las técnicas de detección. Para todas las técnicas, al incrementarse p_e se incrementa también la tasa de acusaciones incorrectas

IA en la Figura 7-13: existe una mayor probabilidad de que el error de la técnica de observación sea interpretado como comportamientos egoístas de los nodos. Sin embargo, también se incrementa la probabilidad de que algunos nodos egoístas (especialmente aquellos con un egoísmo p_s más reducido) no sean detectados, lo cual explica el incremento de *INA* en la Figura 7-14 al aumentar p_e. En cuanto a las distintas técnicas, los resultados presentados demuestran que EFW obtiene el mejor rendimiento en términos de precisión, especialmente para *INA*, con un menor coste en paquetes descartados (Figura 7-15). Las diferencias observadas entre el enfoque Bayesiano y el exponencial se deben al parámetro τ y al promediado que se realiza en la métrica exponencial (ecuación 7-23). Como fue comentado antes, en el enfoque Bayesiano, τ debe ser igual a la suma del error de la técnica de observación p_e más un cierto margen. Por tanto, al incrementar su valor con p_e, los nodos caracterizados por un $p_s<\tau-p_e$ (nodos con un egoísmo muy reducido) son más difícilmente detectados y se incrementa *INA*. Por otro lado, en el caso de las técnicas exponenciales, τ representa la probabilidad de que el nodo esté actuando egoístamente. Reducir τ disminuye *IA*, pero no hace que los nodos con un p_s reducido no sean detectados dado que τ no hace referencia a su egoísmo. El mejor rendimiento de EFW respecto a EIW se debe a que EIW hace el promedio de todos los valores que se obtienen de la función exponencial (ecuación 7-23) tras cada observación, incluidos los calculados al principio con pocas observaciones, que pueden ser más imprecisos. Por otro lado, EFW solo considera los últimos *l* valores calculados y descarta los anteriores, y evita por tanto los cálculos realizados al principio con pocas observaciones[39].

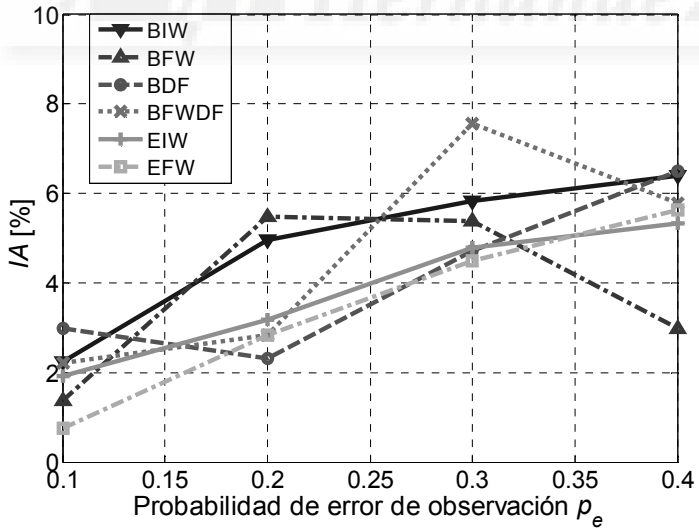


Figura 7-13. Tasa de acusaciones incorrectas en función del error de observación p_e

[39] No obstance, la función exponencial (ecuación 7-23) se calcula siempre con todas las observaciones disponibles.

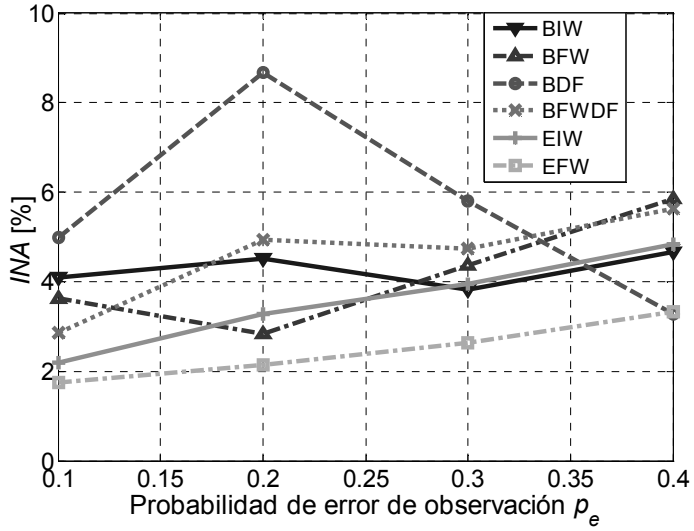


Figura 7-14. Tasa de no acusaciones incorrectas en función del error de observación p_e.

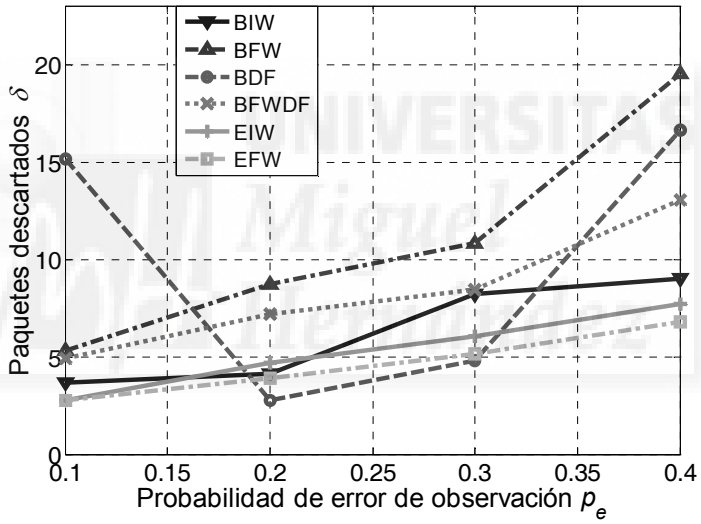


Figura 7-15. Número de paquetes descartados por nodos egoístas antes de su detección δ en función del error de observación p_e.

7.3.4 Sensibilidad al error de estimación de probabilidad de error

Como se ha mencionado a lo largo del capítulo, el rendimiento de las técnicas de detección, tanto las Bayesianas como las exponenciales, depende directamente de la precisión en la estimación del valor del parámetro p_e. Es necesario examinar hasta qué punto influye la precisión de la estimación en la capacidad de las técnicas para realizar estimaciones precisas y rápidas. En las Figuras 7-16, 7-17 y 7-18 se muestran respectivamente los parámetros de rendimiento considerados en este capítulo (*IA*, *INA* y

δ) frente a la desviación del valor estimado de la probabilidad de error $\hat{p}_e$ respecto al valor real de la probabilidad de error de *watchdog*, p_e. Se calculará dicha desviación mediante la siguiente expresión del error relativo:

$$\varepsilon_{pe} = \frac{p_e - \hat{p}_e}{\hat{p}_e} \tag{7-27}$$

Se trata de un error relativo en el que el signo de la desviación es importante, y por tanto no se pueden tomar valores absolutos en la expresión 7-27. Esto se explica porque infravalorar o sobrestimar el error de observación no influye de manera simétrica en los parámetros de rendimiento, tal como aprecia en las figuras siguientes. En el convenio adoptado en la expresión 7-27, cuando se sobrestima la probabilidad de error (la probabilidad de error estimada es mayor que la real), el valor de la desviación ε_{pe} es negativo. Al contrario, si se infravalora la probabilidad de error, entonces quiere decir que la estimación es inferior al valor real y la desviación ε_{pe} es positiva. Teniendo esto en cuenta, se pueden interpretar los resultados mostrados en las figuras siguientes. El valor de la p_e estimada era en todos los casos 0.2, mientras que se varió la p_e real para generar distintos valores de desviación entre ambas. La razón de fijar la p_e estimada y no la real es que el valor de la p_e estimada seleccionado determinaba los valores de los parámetros de configuración τ y l, de acuerdo a las Tablas 7-3 y 7-4. En primer lugar, *IA* e *INA* presentan tendencias opuestas en las Figuras 7-15 y 7-16. Si la probabilidad de error se infravalora, es decir, la p_e real es mayor que la estimada, entonces se corre el riesgo de que ocurran errores en la observación por encima del nivel esperado. Dichos errores pueden provocar que la métrica de detección sobrepase el umbral de acusación τ acorde a la p_e estimada, y por tanto se incrementa la tasa de acusaciones incorrectas *IA*. De manera complementaria, esto hace disminuir el número de ocasiones en que nodos egoístas no son detectados, aumentando por tanto la tasa de no acusaciones incorrectas *INA*. Estas tendencias complementarias se repiten para todas las técnicas de detección evaluadas. Sin embargo, hay que destacar que infravalorar la probabilidad de error es considerablemente más perjudicial que sobrestimarla, especialmente en el caso de la técnica EFW. Como muestra la Figura 7-16, infravalorar en un 25% la p_e real conduce a un aumento de *IA* de hasta el 40%, mientras que sobrestimarla en un 25% no aumenta la *INA* en más de un 10% en la Figura 7-17. La razón de esta diferencia estriba en que los nodos egoístas que más hacen aumentar *INA* son los nodos con un p_s reducido ($0<p_s<0.3$). A pesar de que el conjunto de funciones de de distribución del parámetro p_s considerado, $f_{ps}(x)$, (apartado 7.3.2) es suficientemente amplio, en cada distribución la proporción de nodos con p_s reducido es baja, respecto al total de nodos. Esto hace que *INA* sea poco sensible a las desviaciones en la estimación de p_e. Por otro lado *IA* depende de la proporción de nodos no egoístas ($p_s=0$), la cual suele ser mayor que la de los nodos con p_s reducida, y por ello

es más sensible a las desviaciones en la estimación de p_e, como reflejan las Figuras 7-16 y 7-17.

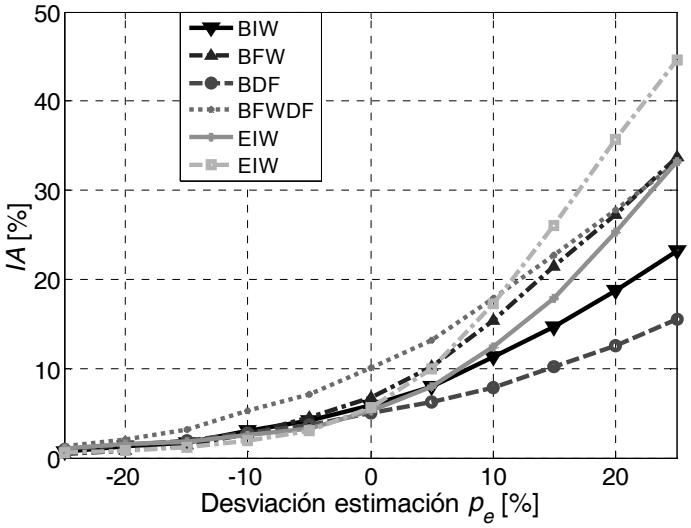


Figura 7-16. Tasa de acusaciones incorrectas *IA* en función de la desviación en la estimación del error de observación p_e.

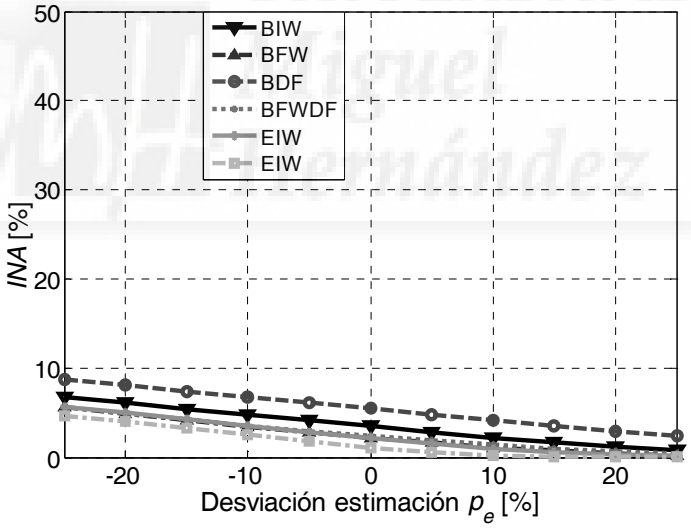


Figura 7-17. Tasa de no acusaciones incorrectas *INA* en función de la desviación en la estimación del error de observación p_e.

En general, la desviación en la estimación del error de observación también influye en la velocidad con que las técnicas son capaces de detectar a los nodos egoístas, como muestra la Figura 7-18. Infravalorar el error de observación aumenta la velocidad de detección, y por ello disminuye el número de paquetes que los nodos egoístas descartan antes de ser detectados. Esto se debe a que infravalorar el error de observación p_e es en cierto modo equivalente a seleccionar un umbral de acusación τ más estricto, y por tanto

las detecciones se realizan antes. El número de paquetes descartados δ para cada técnica, está además directamente relacionado con el número mínimo de observaciones l utilizado en cada técnica, escogido a partir de la Tabla 7-4 a partir del valor de la p_e estimada (0.2). El parámetro l por tanto determina las diferencias en δ que se observan cada técnica en la Figura 7-18.

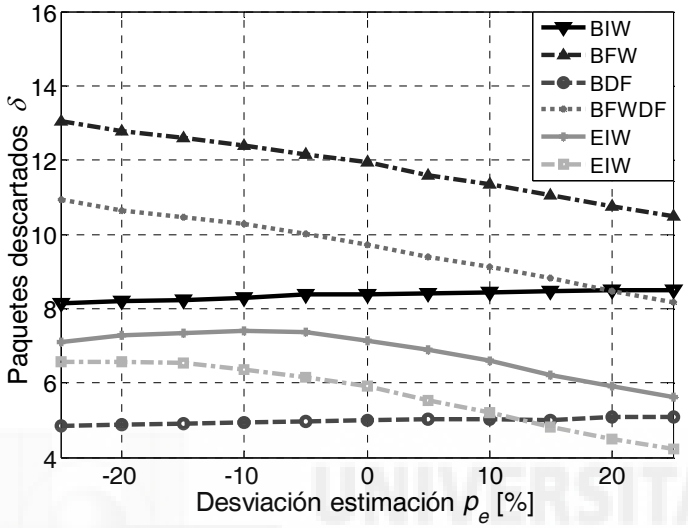


Figura 7-18. Número de paquetes descartados por nodos egoístas antes de su detección δ en función de la desviación en la estimación del error de observación p_e.

7.4 Conclusiones

En los capítulos anteriores se evaluó el rendimiento de distintas técnicas basadas en reputación que empleaban como método de observación la técnica *watchdog*. En el capítulo 5 se mostró que las condiciones de simulación y el canal de propagación tienen una notable influencia en la probabilidad de error de *watchdog*, es decir, en la probablidad de que *watchdog* tome una acción cooperativa como una acción egoísta. Esta incertidumbre en el proceso de observación dificulta considerablemente el funcionamiento de las técnicas de reputación, al aumentar el número de acusaciones incorrectas, y paralelamente disminuir el número de rutas multi-salto disponibles. Por ello, en el capítulo 6 se propusieron técnicas que conseguían mejorar la conectividad de la red al contrarrestar los efectos del error de *watchdog* sobre el número de acusaciones incorrectas.

Sin embargo, hasta ahora se había asumido que los nodos egoístas descartaban siempre los paquetes que debían retransmitir, lo cual no tiene que ser necesariamente cierto. En este capítulo se asume que el nodo egoísta decide para cada paquete de manera aleatoria si lo descarta o no. Con esta generalización resulta más difícil la detección de los

nodos, dado que el comportamiento egoísta del nodo puede estar enmascarado por la probabilidad de error de *watchdog*. Distinguir con precisión si un nodo está descartando paquetes o no, a través de una función métrica que mide el grado de egoísmo, puede requerir realizar una gran cantidad de observaciones. Este compromiso entre la velocidad de detección y la precisión de las decisiones se hace evidente en el capítulo al evaluar analíticamente el funcionamiento de las técnicas de detección más extendidas, que son las técnicas bayesianas. Además, el compromiso dificulta la tarea de seleccionar los valores óptimos de los parámetros de configuración de las métricas de egoísmo, que son principalmente el umbral de acusación τ y el número mínimo de observaciones antes de tomar una decisión, l. Básicamente, el valor de τ plantea un compromiso entre la tasa de acusaciones incorrectas y la tasa de no acusaciones incorrectas, mientras que incrementar l puede incrementar la precisión del proceso de detección pero también lo hace más lento. Para superar estos compromisos, y dada la naturaleza del proceso aleatorio que se ha asumido para el proceso de descarte que realizan los nodos, se ha propuesto un enfoque exponencial basado en la función de distribución binomial. Las técnicas de detección exponencial propuestas se diferencian principalmente de las tradicionales técnicas bayesianas en que hacen explícita la probabilidad de error de la técnica *watchdog* en su métrica de egoísmo. Esto facilita la elección de los valores de los parámetros de configuración de las métricas de egoísmo. Asimismo, las técnicas exponenciales tienen en cuenta todas las observaciones realizadas en el pasado pero a su vez realizan un promediado que tiene como objetivo evitar oscilaciones bruscas de la métrica de egoísmo.

Finalmente, se ha evaluado comparativamente el rendimiento de ambos enfoques, para lo cual fue necesario identificar todos los parámetros que podían influir en el proceso de detección: la distribución del parámetro de egoísmo entre los nodos egoístas de la red, la probabilidad de error de *watchdog*, el número de observaciones máximo, así como los parámetros de configuración de las métricas l y τ. Se realizó un proceso de selección de los valores más adecuados de los parámetros l y τ. Este análisis demostró que una sola configuración de l y τ resultaba ser la más adecuada frente a las variaciones del parámetro p_e en los distintos escenarios propuestos para las técnicas exponenciales. Para las simulaciones, fueron seleccionados escenarios con distintas proporciones del parámetro de egoísmo del nodo p_s, de manera que resultaran representativas de aquellas que más pueden influir en la selección de los valores óptimos de l y τ. Se mostró la variación de los parámetros de rendimiento de precisión y de velocidad de detección frente a la probabilidad de error de *watchdog* p_e (cuyo valor en una red real debe ser estimado por la técnica) y al número de observaciones máximo N. Los resultados presentados demuestran que la técnica exponencial con ventana finita obtiene el mejor rendimiento en términos de precisión, especialmente para la tasa de no acusaciones incorrectas, con un menor coste en paquetes descartados, es decir, con una rapidez mayor. También se ha investigado la

sensibilidad al error en la estimación de la probabilidad de error. Se ha demostrado que es preferible hacer una sobrestimación del valor del parámetro de probabilidad de error de *watchdog*, con el fin de evitar un aumento indeseable de la tasa de acusaciones incorrectas, aunque con ello se tenga que incurrir por otro lado en pequeños incrementos tanto de la tasa de no acusaciones incorrectas como del número de paquetes descartados antes de la detección.

Una vez estudiados los métodos de detección tradicionales Bayesianos, así como el método exponencial propuesto, tanto analíticamente como mediante simulación, el siguiente capítulo aborda la integración de estas propuestas en un entorno de simulación a nivel de sistema considerando un paradigma de red de comunicación no explorado hasta ahora en esta tesis: las redes multi-salto celulares. Esta integración permitirá explorar tendencias que no había sido posible estudiar en el capítulo anterior, y además se podrá apreciar su aplicación en distintas técnicas de reputación, en donde no sólo será importante el proceso de detección, sino que también se tendrá en cuenta el proceso de reacción de cada técnica. Sin embargo, el objetivo fundamental del capítulo será demostrar las considerables ventajas derivadas de la utilización de la infraestructura celular de la red MCN (Multi-salto *Cellular Network*) como sistema de apoyo para las técnicas de reputación y de detección de nodos egoístas. Se mostrará como, aprovechando la capacidad de la red celular, será posible realizar un correcto aislamiento de los nodos egoístas, que no había sido posible realizar hasta ahora. Además, se mostrará la importancia de considerar los distintos niveles de egoísmo en función del parámetro p_s, y cómo en determinados escenarios limitados, no detectar un cierto nivel de egoísmo muy bajo puede ser incluso beneficioso para los nodos cooperativos.

8

Técnicas de reputación en redes multi-salto celular

Recapitulando las líneas principales seguidas en el desarrollo de esta tesis, partíamos en el capítulo 5 del problema de la detección de los nodos egoístas presentes en una red MANET con un doble objetivo: evitar su utilización en las rutas multi-salto en las que se encaminaban los paquetes, y tratar de aislarlos de la red como contrapartida a su falta de cooperación. Con ello se pretende elevar la conectividad de los nodos que contribuyen al mantenimiento de la red (los nodos cooperativos), y disminuir la de los nodos que no lo hacen pero sí se aprovechan de su existencia (los nodos egoístas). En el capítulo 5 se presentaba el funcionamiento y el rendimiento de la técnica de observación *watchdog* en distintas condiciones de operación y de simulación. Se constató que el rendimiento de las técnicas de reputación que utilizaban la técnica *watchdog* descendía notablemente al ser evaluadas en condiciones realistas de simulación, debido a los errores de observación de *watchdog* provocados por errores en el canal de transmisión y colisiones de paquetes. A partir de dicho estudio se propusieron distintas técnicas en el capítulo 6 que buscaban corregir la elevada tasa de acusaciones incorrectas provocadas por el funcionamiento anómalo de *watchdog* que podía afectar considerablemente a la conectividad de la red. El capítulo 7 se centraba en mejorar exclusivamente el proceso de detección de los nodos egoístas, en términos de precisión y rapidez, obviando el proceso de reacción (que se ocupa de la acusación y el aislamiento del nodo egoísta). Además, ampliaba la

generalidad del modelo de nodo egoísta considerado, al introducir el concepto de nodos que no descartaban todos los paquetes de datos que debían retransmitir, sino únicamente una fracción de ellos, de manera aleatoria, lo cual hacía que su comportamiento se confundiera con el error de la técnica de observación *watchdog*. Un aspecto relevante que quedaba por analizar y optimizar es la capacidad de las técnicas de reputación de aislar a los nodos egoístas. Si bien estas técnicas consiguen detectar con mayor o menor rapidez y precisión a los nodos egoístas, esto no se traduce en un aislamiento efectivo de los mismos a nivel global, como se verá en este capítulo, debido a que la información de la identidad de los nodos egoístas no se consigue propagar a todos los nodos de la red, sino que se reduce al ámbito local de los nodos que detectan al nodo egoísta y a algunos nodos vecinos.

Frente a ello, en el presente capítulo convergen algunas de las líneas de investigación seguidas en los capítulos anteriores, al mismo tiempo que se introduce un paradigma de red de comunicaciones cuyas características permiten elevar considerablemente el rendimiento de las técnicas de reputación. En concreto, el objetivo es tratar de aprovechar el potencial de las redes MCN-MR (*Multi-hop Cellular Network – Mobile Relay*) para conseguir una mayor precisión en el proceso de detección y sobre todo, una mayor eficacia en el proceso de aislamiento de los nodos egoístas detectados. La razón para emplear la infraestructura de la red celular como apoyo a la red MANET es aprovechar la complementariedad que ofrecen sus características. La red móvil celular aporta distintas ventajas que permiten solucionar convenientemente algunos problemas de difícil solución en una red MANET pura con presencia de nodos egoístas (identificación única de los nodos, movilidad, etc.). Por otro lado, el diseño de las técnicas de reputación utilizadas debe asegurar un uso eficiente de los recursos de comunicación de la red celular. Para conseguirlo, este capítulo presenta dos técnicas que explotan la capacidad de la infraestructura de red celular para apoyar los procesos de detección de nodos egoístas y su aislamiento. Se comprobará su funcionamiento utilizando las técnicas de detección propuestas y evaluadas en el capítulo 7 (técnicas de detección Bayesianas y exponenciales) y comparando su rendimiento con el de las las técnicas de reputación del capítulo 6 (técnica TEAM junto con las técnicas propuestas).

Si bien es posible encontrar en la literatura algún estudio anterior que ya contemplaba el beneficio de la complementariedad entre redes MANET y redes de área amplia como GPRS [53], las aportaciones del presente trabajo son sustanciales[40]. Concretamente, el trabajo [53] hace hincapié en el diseño de un modelo de reputación que permita a la entidad central distinguir los mensajes de acusación falsos enviados por nodos maliciosos, con el objetivo de causar un daño intencionado a la red, de los mensajes de

[40] El capítulo 2 incluye una descripción más detallada de [53] .

acusación verdaderos que son enviados al detectar un nodo egoísta. Por tanto, el énfasis de dicho trabajo está puesto sobre el problema de la distinción de los mensajes maliciosos creados intencionadamente por ciertos nodos, antes que sobre la cuestión de la incertidumbre introducida en el proceso de detección y acusación por la inexactitud del proceso de observación de *watchdog*. Por ello, cuestiones como la probabilidad de error de observación de la técnica *watchdog* son ignoradas por el estudio, que emplea además unas condiciones de simulación irrealistas, lo cual puede afectar a la precisión de los resultados y las conclusiones obtenidas, tal y como se demostró en el capítulo 5 y se ha podido comprobar en el resto de capítulos. Esta diferencia debe ser considerada, dada la influencia que tiene sobre la conectividad.

En este capítulo se presentan las dos técnicas de reputación para redes MCN propuestas y la evaluación de su funcionamiento. La primera técnica BC (*Broadcast Category*) tiene como objetivo hacer pública la información local de la identidad de los nodos que son detectados como egoístas. Con ello se consigue un verdadero aislamiento global de los nodos que son detectados. Por otro lado, debido al error en el proceso de observación de la técnica *watchdog*, es posible que algunos nodos cooperativos sean incorrectamente acusados y aislados injustamente en toda la red. Para evitar esto, se propone de manera complementaria la técnica SC (*Selfishness Check*), que comprueba tras una detección local si realmente un nodo debe ser o no acusado globalmente. En el último apartado se comprueba el rendimiento de las técnicas en distintos escenarios de simulación y se justifican los resultados obtenidos.

8.1 Técnica BC (*Broadcast Category*)

En las técnicas tradicionales de reputación en redes MANET, la difusión de la información sobre la identidad de los nodos egoístas constituye un desafío. Difundir información entre los nodos que conforman una red MANET convencional puede ser un proceso poco eficiente y consumir una proporción considerable de recursos de comunicación. Algunas técnicas proponen la utilización de agentes para recabar y difundir la información sobre la reputación de los nodos [54]. La principal desventaja de este esquema es la necesidad de la utilización de agentes específicos para tal fin. Otros recurren a una difusión local de la identidad de los nodos que son detectados como egoístas, que generalmente se apoya en un sistema de reputación en el que son necesarias un cierto número de acusaciones por parte de diferentes nodos, que a su vez deben tener una buena reputación, para aislar a un nodo determinado [55]. Aunque los mensajes de acusación/reputación sólo sean difundidos localmente, esto tiene un cierto coste en términos de sobrecarga del canal. Además, es posible que una difusión local de la identidad de los nodos acusados no sea suficiente para aislarlos, debido a la movilidad de

los nodos. La movilidad puede hacer que un nodo egoísta que ya ha sido detectado y aislado en cierta área, continúe descartando paquetes en otra en un momento posterior. Sin embargo, como se puede ver en los ejemplos ilustrados en las Figuras 8-1, 8-2, 8-3 y 8-4 y en los resultados del apartado 8.3.3, la difusión de la identidad de los nodos egoístas es fundamental para aislarlos completamente, y también para evitar la repetición del proceso de detección en cada una de las ocasiones en las que un nodo egoísta aparece como posible retransmisor durante un proceso de establecimiento de ruta.

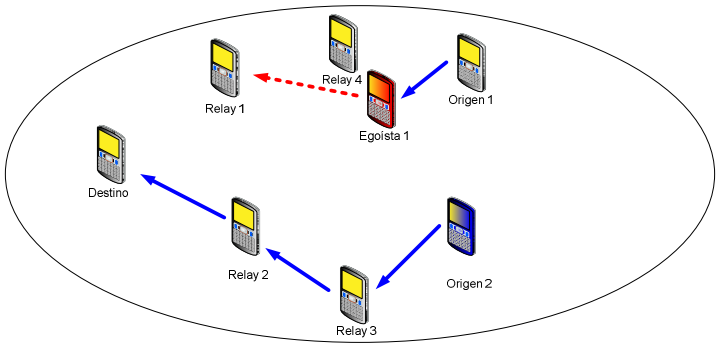


Figura 8-1. Detección local de nodo egoísta.

Considérese la Figura 8-1, en la que se representa un conjunto de nodos formando una red MANET. Dos nodos origen tratan de encaminar paquetes hacia un nodo destino. Para ello emplean alguna técnica de reputación como la de Marti o TEAM[41], en la que la búsqueda de rutas se realiza mediante un protocolo de enrutamiento y para la selección de rutas se tiene en cuenta la información de reputación recabada por la técnica de observación *watchdog*. En el caso del nodo *Origen 1*, la ruta establecida incluye el nodo *Egoísta 1*, dado que todavía no ha sido detectado por el nodo. Tras un cierto número de observaciones por parte del *watchdog* del nodo *Origen 1*, éste detectará el comportamiento egoísta del nodo. Tras deshacer la ruta, en el siguiente establecimiento de ruta seleccionará al nodo *Relay 4* como retransmisor, como refleja la Figura 8-2. Por otro lado, el nodo *Origen 2* ha podido establecer una ruta sin nodos egoístas en la Figura 8-1. En este sentido, la técnica de reputación está actuando correctamente, detectando al nodo y haciendo que el nodo que lo ha detectado lo evite en sus sucesivos procesos de selección de ruta. Sin embargo, debe resaltarse aquí uno de los grandes incovenientes de estas técnicas. Supóngase que el nodo *Egoísta 1* quisiera transmitir sus propios paquetes a través del nodo *Relay 1* hacia el nodo *Destino*. En tal caso no sería posible aislarlo y evitar que *Relay 1* retransmitiera los paquetes paquetes del nodo *Egoísta 1*, dado que *Relay 1* no tiene conocimiento de la detección del nodo *Egoísta 1* por parte del nodo *Origen 1*. Para aislar completamente al nodo egoísta se hace necesario establecer un

[41] Ambas técnicas fueron explicadas en el capítulo 5, dónde además se presentaron los detalles de su implementación en este trabajo.

sistema de reputación en el que se difunda de manera fiable la identidad de los nodos egoístas detectados.

En la Figura 8-2 puede apreciarse otro aspecto deficiente de las técnicas que no incluyen algún sistema de difusión eficaz de la identidad de los egoístas. Cuando el nodo *Egoísta 1* se mueve, el nodo *Origen 2* descubre una ruta alternativa hacia el nodo *Destino*, y lo utiliza como retransmisor en lugar del nodo *Relay 3* (esto podría ocurrir si momentáneamente cayera el enlace entre el *Origen 2* y el *Relay 3*). Dado que el nodo *Origen 2* no tiene conocimiento de la identidad del nodo *Egoísta 1*, tendrá que volver a realizar el proceso de observación y detección que ya ha realizado el nodo *Origen 1*, con la consiguiente pérdida de paquetes que ocasiona este proceso. Igualmente, incluso en el caso en el que la identidad del nodo egoísta se hubiera difundido de manera local, debido a la movilidad de los nodos, es probable que dicha información no hubiera llegado al nodo *Relay 2*. Por tanto, tampoco en este caso el nodo *Egoísta 1* podría ser aislado satisfactoriamente de la red si tuviera paquetes que transmitir como origen.

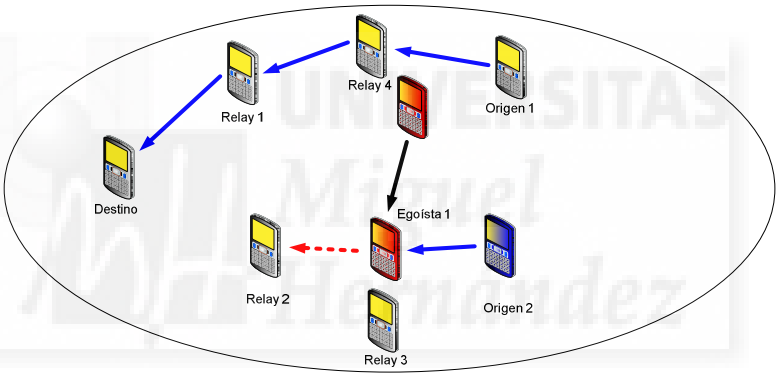


Figura 8-2. Aislamiento local de nodo egoísta.

En este contexto se plantea la utilización de la infraestructura de la red móvil celular como apoyo a la técnica de reputación para la difusión de la identidad de los nodos que son detectados como egoístas. La técnica BC (*Broadcast Category*) consiste en que tras la detección de un nodo como posible egoísta, el nodo precursor (es decir, el nodo que emplea el *watchdog* para vigilar la correcta retransmisión de los paquetes, el nodo *Origen 1* en la Figura 8-1), informa a un servidor central confiable. El servidor central podría implementarse como una entidad de gestión y registro situada dentro de la arquitectura de la red celular, en la parte troncal de la red. Tras recibir el aviso procedente del nodo precursor, el servidor central difunde en modo broadcast un mensaje en el que informa de la identidad del nodo egoísta que ha sido detectado. De esta manera, todos los nodos dentro del área de cobertura (incluso en celdas vecinas en las que también puede difundirse el mensaje de aviso) podrían beneficiarse de esta información, que además serviría para privar completamente al nodo del acceso a la parte multi-salto de la red

MCN como represalia por su comportamiento. Estas consideraciones se ilustran en las Figuras 8-3 y 8-4.

En la Figura 8-3, el proceso de detección del nodo *Origen 1* determina tras un número de observaciones que el nodo *Egoísta 1* está comportándose egoístamente. Si no se recurriera a la infraestructura celular, el nodo simplemente desharía el enlace con el nodo *Egoísta 1* y la ruta, y a continuación evaluaría si es necesario o no establecer una ruta alternativa. Con BC, una vez que el nodo determina que el nodo retransmisor es egoísta, envía un mensaje al servidor central etiquetado como "*Informe comportamiento egoísta*". En dicho mensaje tan solo es necesario incluir la información de la identidad del nodo egoísta. A continuación, el servidor central retransmite en modo *broadcast* dicho mensaje para informar a todos los nodos de la identidad del nodo egoísta detectado. Esto permite que el nodo *Egoísta 1* sea realmente aislado en el momento en que quiera recurrir a la red MCN para transmitir sus propios mensajes, ya que tanto el *Relay 1* como el *Relay 4* sabrían su identidad.

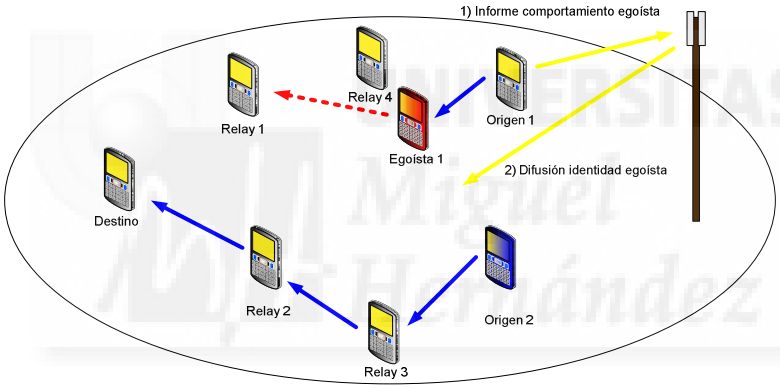


Figura 8-3. Detección local y difusión de identidad de nodo egoísta.

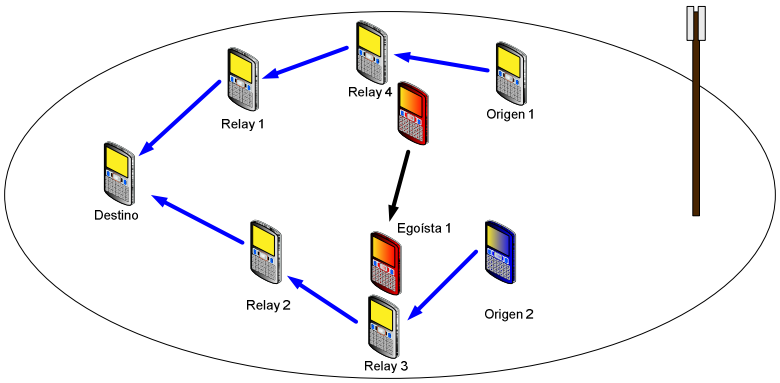


Figura 8-4. Aislamiento global de nodo egoísta.

La Figura 8-4 ilustra los beneficios de la técnica BC. En caso de que el entorno del nodo *Egoísta 1* cambiara por el movimiento del usuario, el nodo *Origen 2* ya estaría prevenido por el mensaje de difusión anterior y no modificaría la ruta establecida,

ahorrándose el proceso de detección que habría tenido que hacer de no haber sido por el mensaje del servidor central, tal y como se mostraba en la Figura 8-2. Por otro lado, el nodo *Egoísta 1* será aislado completamente tal y como se pretendía, dado que todos los nodos conocen su identidad.

A pesar de la considerable ventaja que se obtiene al aprovechar la capacidad de difusión del servidor central, es importante señalar un inconveniente derivado de la inexactitud en la detección de los nodos egoístas. Como se ha podido comprobar a lo largo de la tesis, la técnica de observación de *watchdog* tiene un cierto error de observación, p_e, introducido formalmente en el capítulo 7 y caracterizado como la probabilidad de que un paquete que ha sido realmente retransmitido por el nodo, sea contabilizado como un paquete descartado. Las causas de esta imprecisión pueden derivar de errores de transmisión radio o de colisiones de paquetes. Debido a este error en el proceso de observación, existe la posibilidad de que nodos cooperativos sean acusados incorrectamente de actuar de manera egoísta. Por consiguiente, con la técnica BC estos nodos cooperativos serían aislados completamente de la red MCN. Debido al perjuicio que esto puede causar, tanto al nodo acusado incorrectamente como a la conectividad general de la red multi-salto, es necesario aplicar otras técnicas que mitiguen las consecuencias negativas de la inexactitud de la técnica *watchdog*.

Retomando las técnicas propuestas en el capítulo 6, cuyo objetivo era precisamente aliviar estas consecuencias negativas sobre las técnicas de reputación, consideramos su adaptación para ser empleadas también en el nuevo escenario de una red MCN. En primer lugar, la técnica RAM proponía resetear la reputación y los descartes observados de aquellos nodos de los que cuales se observaba alguna retransmisión. Sin embargo, su aplicación en este escenario podría no ser conveniente, debido a que en este capítulo se asume, como en el capítulo 7, que los nodos pueden tener un comportamiento egoísta aleatorio, modelado por la variable p_s. El parámetro p_s representa la probabilidad de que un nodo descarte un paquete que debe retransmitir. Con esta asunción, la detección de los nodos con un $p_s < 1$ sería más difícil, dado que sería más probable que la reputación de los nodos se fuera reseteando continuamente antes de que se cumpliera la condición de acusación de la técnica de reputación correspondiente. Es por ello que no se ha considerado la mejora de la técnica BC con la introducción de RAM.

Por otro lado, con el objetivo de reducir el número de acusaciones incorrectas, se ha considerado la adaptación de la técnica RFM del capítulo 6. Dicha técnica establecía que se reseteara la reputación degradada del nodo que dejaba de estar dentro del rango de cobertura de otro nodo debido a la caída del enlace. Siguiendo la misma filosofía, se propone que al aplicar la técnica BC se tenga en cuenta si ha habido alguna caída de enlace, y en tal caso, no realizar la difusión de la identidad del nodo detectado como egoísta. Para ello, cuando un nodo detecte la caída de un enlace, envía un mensaje de

aviso de caída de enlace al servidor central. El servidor central establece un tiempo de salvaguarda durante el cual los nodos que forman parte del enlace caído son liberados de que su identidad sea difundida, aún cuando llegue algún mensaje de aviso de detección de egoísta en el que sean acusados. En la presente implementación se ha considerado un tiempo de salvaguarda de un segundo, dado que en simulaciones preliminares se observó que el tiempo transcurrido entre la caída de un enlace y la detección como egoísta del nodo que formaba parte de ese enlace era inferior a un segundo en la mayoría de las ocasiones.

Por último, debe recordarse la tercera de las técnicas propuestas en el capítulo 6, la técnica WM, cuyo objetivo era reducir las acusaciones incorrectas ofreciendo una segunda oportunidad a los nodos antes de ser definitivamente acusados de comportarse egoístamente. Para adaptar la técnica WM y al mismo tiempo aprovechar las potenciales sinergias de la red multi-salto con la capacidad de comunicación del servidor central, en el siguiente apartado se propone una segunda técnica, la técnica SC (*Selfishness Check*), con el mismo objetivo de reducir las acusaciones incorrectas dando una segunda oportunidad al nodo sospechoso.

Un aspecto importante de la utilización de la infraestructura celular consiste en evaluar el coste en términos de carga de señalización introducido por las técnicas propuestas. En una implementación real, los mensajes intercambiados con el servidor central conllevan la necesidad de establecer comunicaciones radio entre los nodos móviles y las estaciones base celulares. Se ha tratado de minimizar la sobrecarga que implica este intercambio de mensajes. En primer lugar, únicamente se generan mensajes de aviso cuando la técnica de detección determina de modo local que un nodo debe ser acusado. Por tanto, uno de los requisitos será aplicar técnicas con un alto grado de precisión en sus acusaciones (es decir, que del total de acusaciones que realicen, la mayoría sean acusaciones correctas). Por otro lado, difundir la identidad de los nodos acusados también contribuye a reducir los mensajes de acusación desde el móvil hasta el servidor central, dado que los nodos que son acusados no vuelven a ser acusados otra vez (no vuelven a actuar como retransmisores). Por último, la adaptación de la técnica RFM también contribuye a reducir el número de transmisiones *broadcast* desde el servidor central, al no realizarse la difusión de la identidad de los nodos que son detectados cuando formaban parte de un enlace caído. No obstante, el número de mensajes de aviso y de transmisiones broadcast también ha sido parametrizado durante este estudio para ser evaluado en los resultados.

Antes de presentar la técnica SC, la Figura 8-5 ilustra esquemáticamente el funcionamiento de la técnica BC.

Técnica BC
Evento detección local de egoísta (en nodo local) "Modo salvaguarda" activado para nodo sospechoso? → SÍ: Ignorar evento detección local NO: Enviar alarma local a entidad central
Evento recepción mensaje alarma local (en nodo central) "Modo salvaguarda" activado para enlace sospechoso? → SÍ: Ignorar evento detección NO: Difundir mensaje acusación global
Evento recepción mensaje acusación global (en nodo local) Categoría nodo pasa a egoísta
Evento recepción aviso de caída de enlace (en nodo central) Categoría nodos enlace pasa a "modo salvaguarda"

Figura 8-5. Pseudocódigo de la técnica BC.

8.2 Técnica SC (*Selfishness Check*)

Como ya se ha anticipado en el apartado anterior, a pesar de la gran ventaja que supone poder aislar completamente a los nodos egoístas, hay una contrapartida como consecuencia de la imprecisión del proceso de observación de *watchdog* al ser utilizada la técnica BC: algunos nodos cooperativos pueden ser detectados incorrectamente y ser aislados injustamente de manera global. Esta circunstancia exige que se intente reducir al mínimo el número de acusaciones incorrectas realizadas. Para ello se propone una técnica que compruebe si realmente el nodo ha dejado de transmitir los paquetes que debería haber retransmitido o no. Esta comprobación adicional es una oportunidad para que el nodo pueda librarse de ser acusado, y en este sentido, puede entenderse como una adaptación de la filosofía de la técnica WM propuesta en el capítulo 6. La técnica WM, presentada en el apartado 6.2, proponía que los nodos que eran detectados como egoístas no fueran acusados en ese mismo instante, sino que recibían una nueva oportunidad para recuperar su reputación, que podía haberse degradado por el error en el proceso de observación *watchdog*. Esa segunda oportunidad consistía en que, si tras un nuevo reestablecimiento del enlace el nodo transmitía correctamente los paquetes, su reputación era recobrada. Si por el contrario, comenzaba otra vez a descartar paquetes, era acusado definitivamente.

La técnica SC (*Selfishness Check*) consiste igualmente en otorgar una segunda oportunidad a los nodos que han sido detectados como egoístas para que la detección no se materialice inmediatamente y el nodo sea acusado globalmente (con la técnica BC, aunque también puede aplicarse la técnica SC por separado) y aislado de la red, teniendo en cuenta que puede tratarse de una detección errónea. Para ello, se aprovecha de la capacidad de supervisión del proceso de detección que puede ejercer el servidor central con la ayuda de los nodos de la red.

La técnica SC requiere la cooperación de los nodos y la entidad central en el proceso de vigilancia, detección y aislamiento de los nodos egoístas. La técnica se ejecuta en varios de estos procesos. En primer lugar, durante el proceso de vigilancia cuando un nodo transmite paquetes a través de una ruta multi-salto, y cuando un nodo recibe paquetes retransmitidos por otros nodos. En segundo lugar, durante el proceso de detección, cuando un nodo detecta que otro puede estar comportándose egoístamente e informa de ello a la entidad central. En tercer lugar, cuando la entidad central, antes de acusar definitivamente al nodo, comprueba si realmente el nodo se ha comportado egoístamente, consultando a los nodos que participaban en el enlace bajo sospecha. Todos estos procesos se explican con la ayuda de la Figura 8-6.

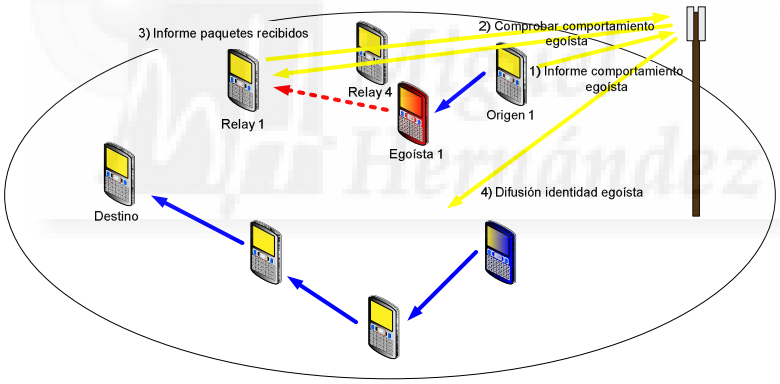


Figura 8-6. Proceso de comprobación de técnica *Selfishness Check*.

En la Figura 8-6 el nodo *Origen 1* está transmitiendo hacia el nodo *Destino* a través de una ruta multi-salto que atraviesa el nodo *Egoísta 1*, del cual todavía no conoce su comportamiento, y el nodo *Relay 1*. El proceso de vigilancia de la técnica SC se ejecuta mientras los nodos transmiten paquetes a través de rutas multi-salto. En concreto, el nodo *Origen 1* tiene un registro de paquetes enviados que contabiliza el número de paquetes que el nodo *Egoísta 1* debería haber retransmitido (n)[42] y el número de paquetes que ha observado como no retransmitidos (α_n), para lo cual empleará la técnica *watchdog*. De esta manera, la información de la técnica *watchdog* sirve por un lado para poder evaluar

[42] La notación utilizada para estos parámetros coincide con la del capítulo 7, para mantener la uniformidad.

las métricas de egoísmo (presentadas durante el capítulo 7) que permiten decidir si un nodo debe o no ser acusado, y por otro para actualizar el registro que podrá ser utilizado posteriormente por otro proceso de la técnica SC. El registro de paquetes enviados se actualiza después de cada observación de *watchdog* y se resetea cada vez que ocurre una caída del enlace. Igualmente, cada nodo que recibe paquetes retransmitidos por otro nodo también lleva un registro paralelo de paquetes recibidos. En el diagrama de la Figura 8.6, el nodo *Relay 1* lleva un registro de los paquetes recibidos n_R que han sido retransmitidos por el nodo *Egoísta 1*. Dicho registro se inicia cuando se establece la ruta, se actualiza cuando se recibe algún paquete, y se borra cuando el enlace se cae o la ruta se deshace. Supóngase que el nodo *Origen 1*, empleando alguna de las métricas del capítulo 7, determina que el nodo *Egoísta 1* se está comportando egoístamente. Esto hará que genere un informe de comportamiento egoísta (paso 1 en la Figura 8-6), en el que se transmite la siguiente información a la entidad central a través del interfaz radio celular:

- identidad del nodo precursor (*Origen 1*),
- identidad del nodo retransmisor (*Egoista 1*),
- identidad del nodo sucesor (*Relay 1*),
- número de paquetes transmitidos en total (n),
- número de paquetes descartados por el nodo retransmisor (α_n)[43].

Dicha información es obtenida a partir del registro de paquetes enviados del nodo precursor (*Origen 1*). La entidad central, tras recibir el mensaje de informe de comportamiento egoísta transmitirá un mensaje de comprobación de comportamiento egoísta (paso 2 en la Figura 8-6) al nodo sucesor, en este caso el nodo *Relay 1*. En este mensaje hará una petición al nodo sucesor *Relay 1* en la que solicitará la información del número de paquetes que realmente ha recibido del nodo retransmisor *Egoísta 1*. En concreto, el mensaje de informe de comportamiento egoísta se compone de los siguientes datos:

- identidad del nodo precursor (*Origen 1*),
- identidad del nodo retransmisor (*Egoista 1*).

A continuación, el nodo sucesor (*Relay 1*) consulta su registro de paquetes recibidos y extrae el número de paquetes recibidos a través de la ruta determinada por los nodos *Origen 1* y *Egoísta 1* y responde al servidor central con un mensaje de informe de paquetes recibidos (paso 3). Dicho mensaje contiene la siguiente información:

[43] α_n hace referencia al número de paquetes que el nodo precursor observa como descartados por el nodo retransmisor, que es la información de la que dispone el nodo precursor, ya que no puede saber exactamente el número de paquetes descartados.

- identidad del nodo precursor (*Origen 1*),
- identidad del nodo retransmisor (*Egoista 1*),
- identidad del nodo sucesor (*Relay 1*),
- número de paquetes recibidos en total (n_R).

Una vez que el servidor central dispone de esta información, evaluará la diferencia entre el número de paquetes que debería haber recibido el nodo sucesor (n) y el número de paquetes que realmente ha recibido (n_R). Se establece un cierto margen de error ε_N, dado que algunos de los paquetes pueden no haber sido recibidos correctamente por el nodo sucesor por otras causas que no son el egoísmo del nodo retransmisor (por ejemplo, errores de transmisión en el enlace entre el nodo retransmisor y el nodo sucesor, caídas de canal o de ruta, etc.). En la presente implementación se ha empleado un margen de error de dos paquetes[44].

$$n - n_R \geq \varepsilon_R \tag{8-1}$$

Si la resta de n y n_R es mayor o igual que el margen, como indica la ecuación 8-1, entonces el nodo es definitivamente acusado: su identidad se comunica bien en un mensaje *unicast* dirigido al nodo precursor (si no se emplea la técnica BC), o bien se difunde por todo el área de cobertura de la entidad central. Este mensaje correspondería al paso 4 en la Figura 8-6, y contiene la siguiente información:

- identidad del nodo egoísta (*Egoista 1*),
- estimación global de la probabilidad de error (p_{eg}).

La p_{eg} es la estimación de la p_e, que todos los nodos en la red tomarán como referencia para hacer los correspondientes cálculos de las métricas de detección (Bayesianas o exponenciales), en caso de que se emplee la técnica BC. Cuando se emplea la técnica BC, el servidor central informa de la estimación de p_e que deben usar los nodos. Si no se emplea la técnica BC; cada nodo utiliza como estimación de la p_e un valor local que debe ser configurado previamente, p_{el}. Por otro lado, la p_{eg} puede ser fija[45] o variable. En caso de que sea variable, su valor se actualiza después de cada proceso de comprobación de la técnica SC (ver Anexo A-II), a partir de los datos recabados durante el proceso de

[44] Este valor se ha adoptado de manera provisional. El valor óptimo a escoger es un compromiso entre el número de acusaciones y no acusaciones incorrectas y debe considerar factores del entorno de la red que afecten a la probabilidad de error de paquete de la transmisión radio.

[45] En el Anexo II se comentan las soluciones más inmediatas para implementar la estimación de la p_e que necesitan las métricas de detección Bayesianas y exponenciales. La más sencilla es utilizar un valor constante a lo largo de la simulación. Una solución adaptativa consiste en utilizar algún método de estimación de los que se pueden encontrar en la literatura. Otra alternativa, aprovechando la capacidad de la entidad central celular, consiste en actualizar el valor de la estimación de la p_e tras cada proceso de comprobación de egoísmo de la técnica SC como se describe en esta sección.

comprobación de egoísmo de la técnica SC. En primer lugar, se calcula la probabilidad de error promedio p_{ea}, que es una estimación de la p_e experimentada durante el proceso de envío de paquetes que desencadenó el proceso de comprobación de egoísmo (ver Figura 8.6). Para el cálculo de p_{ea} se emplea la siguiente expresión:

$$p_{ea} \approx \frac{n_R - (n - \alpha)}{n_R} = 1 - \frac{n - \alpha_n}{n_R} \tag{8-2}$$

Los valores n_R, n y α_n corresponden a los parámetros de información proporcionados a la entidad central por parte de los nodos precursor y sucesor durante el proceso de comprobación, y estos a su vez se extraen de los registros de paquetes enviados y paquetes recibidos. La expresión 8-2 se ha obtenido despejando la p_e en las expresiones siguientes que describen la relación entre los parámetros y se han tomado a partir de la expresión 7.1 en el apartado 7.1.1:

$$\begin{aligned} n_R &\approx n(1 - p_s) \\ \alpha_n &\approx n(p_s + p_e - p_s p_e) \end{aligned} \tag{8-3}$$

Las expresiones en 8-3 relacionan el número de paquetes total que deberían haberse transmitido (n) con los parámetros de paquetes recibidos por el sucesor (n_R) y paquetes observados como descartados (α_n) a través de las probabilidades de error de observación del *watchdog* p_e y de descarte del paquete por parte del nodo retransmisor p_s, como se explica en el apartado 7.1[46]. Eliminando en el sistema el parámetro p_s y despejando p_e se llega a la expresión 8-2. La p_{ea} calculada sirve para actualizar el valor de la p_{eg}. Por un lado, el valor de la p_e real de cada transmisión será altamente variable, y será inevitable cometer un cierto error cuando se estima su valor. Dado que la p_{ea} calculada por este método reflejará esta variabilidad y puede tomar valores muy diferentes entre sí, se propone la siguiente heurística para actualizar el valor de la p_{eg}:

$$p_{eg1} = (1 - \xi) p_{eg0} + \xi p_{ea} \tag{8-4}$$

donde p_{eg1} representa el valor de la p_{eg} actual, p_{eg0} representa el valor de la p_{eg} anterior y ξ es un coeficiente que define la variabilidad que se quiere dar al parámetro de p_{eg}. Cuanto más próximo a 1, más variará en cada actualización el valor de p_{eg}, mientras que cuanto más próximo a 0, más estable será, pero más lenta será la convergencia al valor

[46] Las equivalencias expresadas en la ecuación 8-3 no son igualdades sino aproximaciones, ya que los valores de la realización concreta (a_n, n_r y n) del proceso de detección pueden variar con cada realización, mientras que p_s y p_e corresponden a los valores parámetricos del proceso, que se suponen constantes. Las equivalencias expresadas sí podrían convertirse en igualdades, pero sólo en promedio.

real de p_e. En las técnicas Bayesianas, la estimación p_{eg} servirá para seleccionar los parámetros de configuración de las métricas: τ y l (ver el capítulo 7 y el apartado 8.3.8). En las técnicas exponenciales, la estimación p_{eg} sirve para poder calcular correctamente la función métrica exponencial (ver apartado 7.2). Por tanto, en ambos casos se hace necesario contar con alguna estrategia que permita obtener una estimación adecuada de la p_e. El error cometido al realizar esta estimación también influirá en el número de acusaciones incorrectas y de no acusaciones incorrectas, parámetros que serán evaluados en los siguientes apartados. La Figura 8-7 muestra el pseudocódigo de la técnica SC.

Técnica SC
Evento detección local de egoísta (en nodo local) Enviar alarma local a entidad central
Evento recepción / envío mensaje datos (en nodo local) Actualizar correspondiente registro
Evento recepción mensaje alarma local (en nodo central) Solicitar información registro nodo sucesor Comprobación concordancia mensajes recibidos Nodo retransmisor debe ser acusado? SÍ: Calcular probabilidad de error Enviar mensaje acusación

Figura 8-7. Pseudocódigo de la técnica SC.

El objetivo de la técnica SC es minimizar el número de veces en que un nodo cooperativo es acusado de comportamiento egoísta, sin provocar por otro lado que nodos que han sido detectados como egoístas no sean finalmente acusados. El coste de aplicar esta técnica será principalmente en términos de mensajes intercambiados por el interfaz celular entre los nodos y la entidad central. Durante el proceso de evaluación de resultados se prestará atención a estos parámetros para cuantificar el impacto de aplicar la técnica SC, bien de manera aislada o bien en combinación con la técnica BC, modalidad en la que se espera obtener el máximo rendimiento: una elevada conectividad para los nodos cooperativos y una conectividad muy reducida para los nodos más egoístas.

Las técnicas BC y SC también pueden ser aplicadas conjuntamente. De hecho, ambas presentan características complementarias. Mientras BC aporta la posibilidad de hacer pública la identidad de los nodos que son detectados como egoístas, la técnica SC tiene como objetivo corregir aquellas acusaciones que puedan ser erróneas y que al aplicar la técnica BC resultan en un aislamiento muy perjudicial de nodos que en realidad son

cooperativos. Para entender mejor el funcionamiento de la técnica que engloba a BC+SC, la Figura 8-8 muestra el pseudocódigo de ambas empleadas simultáneamente.

Técnicas BC+SC
Evento recepción / envío mensaje datos (en nodo local) Actualizar correspondiente registro
Evento recepción aviso de caída de enlace (en nodo central) Categoría nodos enlace pasa a "modo salvaguarda"
Evento detección local de egoísta (en nodo local) Modo salvaguarda activado para nodo sospechoso? → SÍ: Ignorar evento detección local NO: Enviar alarma local a entidad central Enviar alarma local a entidad central
Evento recepción mensaje alarma local (en nodo central) Modo salvaguarda activado para enlace sospechoso? → SÍ: Ignorar evento detección local NO: Solicitar información registro nodo sucesor Solicitar información registro nodo sucesor Comprobación concordancia mensajes recibidos Nodo retransmisor debe ser acusado? → SÍ: Calcular probabilidad de error Enviar mensaje acusación global NO: Reajustar probabilidad de error
Evento recepción mensaje acusación global (en nodo local) Categoría nodo pasa a egoísta

Figura 8-8. Pseudocódigo de la técnica BC+SC.

8.3 Evaluación experimental

Para la evaluación experimental de las técnicas propuestas, se llevó a cabo una implementación en ns-2 de la parte del interfaz radio celular con el objetivo de dotar al simulador de la capacidad para evaluar los resultados que se presentan en este capítulo. En la implementación se amplió la funcionalidad de la herramienta de simulación ns-2 utilizada en capítulos anteriores, para poder simular la parte celular de la red MCN-MR.

En concreto, se determinó un criterio basado en la calidad del enlace radio celular para determinar si un nodo actúa o no como nodo híbrido. Los nodos híbridos seleccionados de esta manera son los encargados de intercambiar los paquetes de datos procedentes de ambas redes, entre el interfaz radio 802.11 y la red celular HSDPA y viceversa (si bien todos los nodos conservan la capacidad de comunicarse con la entidad central celular a través del interfaz radio celular). Los detalles de la implementación realizada se presentan en el Anexo A-I.

8.3.1 Métricas de rendimiento

El objetivo de las técnicas presentadas en este capítulo es aprovechar la capacidad de la infraestructura de la red celular para obtener un aislamiento consistente de los nodos que no cooperen en el mantenimiento de la red multi-salto, frente a aquellos nodos que sí cooperan y que deberían obtener la máxima conectividad posible. Para medir el grado de aislamiento y de conectividad se empleará el parámetro PDR (*Packet Delivery Ratio*) que ya ha sido presentado y utilizado en capítulos anteriores. PDR hace referencia al porcentaje de paquetes recibidos correctamente frente al total de paquetes transmitidos. Es un parámetro de rendimiento que proporciona una medida adecuada de las prestaciones de las técnicas de reputación evaluadas, permite comparar entre sí las distintas técnicas, e indirectamente recoge las influencias de importantes factores que también pueden ser evaluados por separado para justificar las tendencias observadas. Los paquetes que no son entregados correctamente en el nodo destino pueden haberse perdido por distintas causas: paquetes descartados sin ruta, descartados por nodos egoístas, descartados por caída de enlace y descartados por su origen no seguro. Los paquetes descartados sin ruta son los que no se han podido retransmitir porque el protocolo de enrutamiento no ha hallado una ruta válida, o bien la ruta por la que se estaban transmitiendo deja de ser válida (algún enlace caduca o se cae, se detecta un nodo egoísta, etc.). En el caso de que se aplique alguna técnica de reputación, esto puede deberse al hecho de que una alta proporción de los nodos hayan sido acusados de egoísmo. Los paquetes descartados por nodos egoístas son aquellos que al alcanzar en la transmisión multi-salto un nodo egoísta en la ruta, son descartados. Los paquetes descartados por caída de enlace son aquellos paquetes que esperaban en el buffer de una ruta a ser transmitidos, y son descartados cuando el enlace se cae. Los paquetes descartados por su origen no seguro son aquellos que son descartados por un nodo al detectar que provienen de algún nodo acusado de actuar egoístamente. En resumen, para justificar los valores de PDR se debe evaluar la causa que motiva que los paquetes sean descartados, y ver si predominan los paquetes descartados por nodos egoístas (lo cual puede estar relacionado con una técnica de reputación que no detecta y aisla correctamente a los nodos egoístas) o los paquetes descartados sin ruta. En caso de que predominen los paquetes descartados

sin ruta, puede deberse a distintas circunstancias: que la proporción de nodos no egoístas sea en ocasiones demasiado baja como para poder establecer rutas seguras, o bien que la técnica de reputación obtenga un error por acusaciones incorrectas (*IA*) demasiado elevado, motivando la escasez de rutas libres de nodos egoístas conocidos. Un elevado nivel de paquetes sin ruta también puede estar justificado por una reducida densidad de nodos.

La aplicación de las técnicas propuestas tiene un coste en términos de mensajes de señalización transmitidos por el interfaz celular. Se cuantifica el número de mensajes generados por las distintas mejoras, por separado y de forma conjunta. Además también se muestran separados en función del resultado de las acusaciones o no acusaciones realizadas por las técnicas a consecuencia de los mensajes. Los mensajes se dividen en distintas categorías en función de si culminan o no en una acusación del nodo retransmisor, y de si el nodo retransmisor era realmente o no egoísta. De esta manera, se podrá observar cuál es el porcentaje de nodos acusados incorrectamente y aislados a nivel global con la técnica BC, y cuántos de estos nodos que serían acusados sin SC, son redimidos por la aplicación de esa técnica.

Para poder justificar las tendencias seguidas por la métrica del PDR se evalúan otros parámetros más específicos. En concreto, para analizar el funcionamiento del proceso de detección se han evaluado las métricas principales: la tasa de acusaciones (correctas e incorrectas), el número total de acusaciones, y velocidad de detección δ. La tasa de acusaciones es el cociente entre el número de nodos que han sido acusados y que tienen un determinado grado de egoísmo p_s y el número total de nodos en el escenario con ese grado de egoísmo. En el caso de que p_s=0, se trata de la métrica *IA* (*Incorrect Accusations*) ya estudiada en el capítulo 7. El objetivo de las técnicas de reputación es obtener un reducido valor de *IA*, al mismo tiempo que para p_s>0 la tasa de acusaciones correctas debe ser lo más alta posible[47]. Por otro lado, el número total de acusaciones refleja el número de acusaciones totales que fueron realizadas a lo largo de la simulación. Los resultados de esta métrica reflejan el número de acusaciones que las técnicas de reputación aplicadas necesitan para aislar a los nodos. Esto permitirá evidenciar una de las diferencias más notables entre el aislamiento global conseguido por la técnica BC y el resto de técnicas. La técnica BC necesitará un número mucho menor de acusaciones totales, dado que cada acusación tiene un ámbito global y hace que el nodo acusado no vuelva a participar en el enrutamiento de paquetes y por tanto tampoco pueda volver a ser acusado. Finalmente, el parámetro δ mide la capacidad de detectar con rapidez a los nodos egoístas. El objetivo es obtener un δ reducido, ya que cuanto menor es δ, menos

[47] En términos porcentuales, el porcentaje de acusaciones correctas se podría expresar en función del parámetro *INA* definido anteriormente como 100 – *INA*. El objetivo de minimizar la tasa de *INA* es equivalente a maximizar el porcentaje de acusaciones correctas.

paquetes descartan los nodos egoístas antes de ser detectados. δ, al igual que *INA*, se ve afectado también por el parámetro p_s. Cuanto mayor es el egoísmo (mayor es p_s), más rápidamente son detectados los nodos, y por tanto, a pesar de que descartan una proporción mayor de paquetes, son detectados antes y el δ resultante es menor.

Las técnicas de reputación se componen de dos módulos fundamentales: monitorización y reacción. Además de analizar el proceso de detección, también deben analizarse los resultados del proceso de reacción. El proceso de reacción tiene una función doble: aislar adecuadamente a aquellos nodos que han sido detectados como egoístas, y evitar que los nodos egoístas descarten paquetes. En cuanto a la primera función, la capacidad de aislamiento de las técnicas se analiza con dos métricas: el PDR de los nodos egoístas (a menor PDR de los nodos egoístas, mayor capacidad de aislamiento), y el porcentaje de paquetes descartados sin ruta de los nodos egoístas (para demostrar que el reducido PDR obtenido por los nodos egoístas se debe a que no son capaces de encontrar una ruta por estar aislados por el resto de los nodos). Respecto a la segunda función, se deberá examinar el porcentaje de paquetes descartados por nodos egoístas en función del grado de egoísmo del nodo que descarta el paquete.

8.3.2 Escenarios de evaluación

En este estudio se ha empleado de nuevo la plataforma de simulación ns-2 descrita en el capítulo 4 para evaluar las propuestas presentadas en este capítulo. Se realizaron simulaciones a nivel de sistema emulando el funcionamiento de una red móvil inalámbrica multi-salto. Se ha incorporado el mecanismo descrito en el anexo A-I para poder simular el enrutamiento de los paquetes en la red híbrida teniendo en cuenta el enlace celular entre los nodos y la estación base. Las condiciones de simulación son similares a las descritas en el capítulo 6 y se recogen en la Tabla 8.1.

Para realizar una evaluación más exhaustiva del funcionamiento de las técnicas propuestas, se han llevado a cabo simulaciones en dos escenarios con condiciones diferentes, denominados escenario I y escenario II. En cada uno se han variado dos parámetros de configuración que permiten comparar el rendimiento de las técnicas de reputación ante distintos niveles de conectividad y distintas proporciones de nodos egoístas en la red. Los dos parámetros son la potencia de transmisión en el interfaz radio 802.11 y la distribución del parámetro p_s entre los nodos de la red. El escenario I, con una conectividad más restringida, emplea una potencia de transmisión de 17dBm y una proporción de nodos egoístas del 50%, entre los cuales el parámetro p_s se distribuye uniformemente en los valores $\{p_s$=0.1,0.2,0.3…,1.0$\}$, es decir, existen el mismo número de nodos con cada nivel de p_s. En el escenario II, la conectividad se ve favorecida por una

potencia de transmisión mayor (20dBm) y por una proporción menor de nodos egoístas (20%), entre los cuales el nivel de egoísmo p_s también es uniformemente distribuido.

Parámetro	Valor
Tipo escenario	Manhattan 8x8 edificios
Dimensiones	1800x1800m^2
Modelo movilidad	*Random Walk Obstacle* [31]
Número nodos	405
Número estaciones base	1
Densidad nodos	1 nodo cada 80m
Interfaz radio transmisiones ad-hoc	802.11a en banda de 5.8GHz
Potencia transmisión	17/20 dBm [esc. I / esc. II]
Modelo propagación canal radio	Urbano micro-celular WINNER [26]
Distinción propagación LOS/NLOS	Sí (ver sección 4.2.2)
Modelado capa MAC	CSMA/CA, DCF y RTS/CTS.
Modelado efectos de capa física	LUT de *Packet Error Rate* (PER)[48]
Modelo tráfico	Tráfico web [29]
Porcentaje nodos con sesiones activas	15%
Porcentaje nodos egoístas	50%/20% [esc. I / esc. II]

Tabla 8-1 Configuración de parámetros de simulación[49].

8.3.3 Técnicas de referencia

Se han escogido distintas técnicas que sirven como referencia de rendimiento con el cual comparar el obtenido al aplicar cada una de las propuestas de este capítulo. La Figura 8-9 representa el PDR promedio experimentado por los nodos con diverso grado de egoísmo p_s para las distintas técnicas utilizadas como referencia, en el escenario I, mientras que la Figura 8-10 corresponde al escenario II. La etiqueta "Sin detección" hace referencia a la utilización del algoritmo de enrutamiento básico, DYMO, sin la asistencia de ningún tipo de técnica de reputación. Constituye un límite inferior de rendimiento, en el que no se establecen tablas de reputación, sino que a la hora de establecer las rutas cualquier nodo que esté dentro del alcance de los otros nodos puede participar. En este

[48] Consultar la sección 4.2.2
[49] Esc. I y esc. II se refieren al escenario I y al escenario II comentados en el texto.

escenario, tanto los nodos egoístas como los cooperativos tienen unas probabilidades similares de establecer rutas con algún nodo egoísta, y no tienen ninguna posibilidad de evitarlo, por lo cual obtienen un rendimiento en términos de conectividad (PDR) similar, tal y como puede apreciarse en las Figuras 8-9 y 8-10. En el otro extremo está la técnica etiquetada como PD (*Perfect Detection*)[50], que representa una técnica de reputación ideal en la que cada nodo conoce de antemano la identidad de los nodos egoístas, y por tanto son perfectamente aislados con un PDR nulo, tal y como se aprecia en las Figuras 8-9 y 8-10. Puede apreciarse en la Figura 8-9 además una diferencia sustancial entre los escenarios considerados. En el escenario I, los dos factores que propician una menor conectividad (una densidad mayor de nodos egoístas y una potencia de transmisión menor) hacen que el máximo PDR alcanzable por los nodos cooperativos, aplicando la técnica PD, sea incluso menor que cuando no se emplea ninguna técnica de reputación. Este hecho paradójico se explica porque ambos factores limitan la conectividad de la red, especialmente al considerar la técnica PD, que aísla completamente a los nodos egoístas, independientemente de su grado de egoísmo. Sin embargo, si no se aplica ninguna técnica de reputación, sí que se llegarán a utilizar los nodos con un grado de egoísmo más reducido, y esto mejora en conjunto la conectividad de la red. De ahí esa diferencia en el PDR de los nodos cooperativos al comparar ambas técnicas. Por otro lado, en el escenario II (Figura 8-10), donde la potencia es mayor y la densidad de nodos egoístas menor, la limitación en la conectividad es menor y por ello la técnica de reputación PD consigue un PDR de los nodos cooperativos mayor.

Otra conclusión paradójica que puede apreciarse en las Figuras 8-9 y 8-10 es que la técnica de reputación TEAM, y la técnica TEAM con la mejor de las técnicas propuestas en el capítulo 6, etiquetada como "TEAM + WRAM", tampoco consiguen aislar a los nodos egoístas, al igual que ocurría al no emplear ninguna técnica de detección. TEAM + WRAM emplea las mejoras WM y RAM (ver capítulo 6) junto con la técnica TEAM. El PDR obtenido por TEAM revela que se reduce la conectividad para todos los nodos respecto al caso sin detección. Esto era esperable, ya que en TEAM habrá ciertos nodos que se detecten como egoístas y que no podrán ser tenidos en cuenta para establecer rutas, con la consiguiente reducción de conectividad en la red. Sin embargo, lo que más llama la atención es que los nodos egoístas tienen un PDR similar al de los nodos cooperativos en la técnica TEAM y en TEAM+WRAM. Al aplicar las mejoras, se aprecia que las mejoras WRAM consiguen elevar el PDR de los nodos cooperativos en la técnica TEAM, pero también elevan el PDR de los nodos egoístas. Este incremento en el PDR al aplicar las mejoras a TEAM se aprecia mejor en el escenario II (Figura 8-10). Sin embargo, como se mencionaba en el comienzo de este capítulo, sin la asistencia del servidor central, el

[50] Esta técnica idealista ya fue empleada como referencia en el capítulo 6

aislamiento de los nodos egoístas es difícil de alcanzar. Esto ocurre, a pesar de que otros parámetros que se muestran posteriomente revelan que tanto TEAM como TEAM+WRAM detectan nodos egoístas (ver sección 8.3.6). Pero las detecciones son locales y por tanto los nodos egoístas pueden utilizar otros nodos distintos a los que les acusan para realizar sus transmisiones. Para tratar de alcanzar un aislamiento de nodos egoístas más parecido al que refleja la técnica PD, es necesario acudir a la asistencia del servidor central, tal como se muestra en los apartados siguientes.

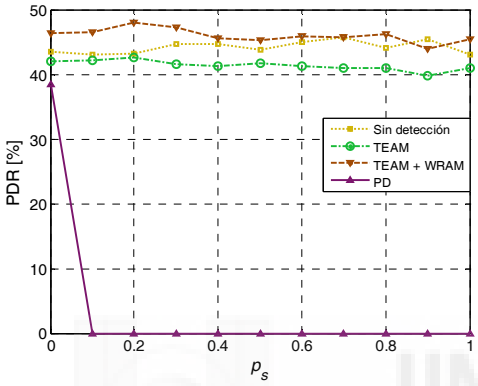


Figura 8-9. PDR de técnicas de referencia en escenario I.

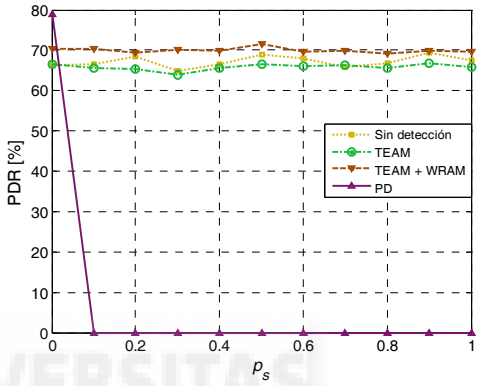


Figura 8-10. PDR de técnicas de referencia en escenario II.

8.3.4 Técnicas centralizadas en redes MCN

Las Figuras 8-11 a 8-18 muestran el efecto sobre la conectividad del uso de un servidor centralizado. Para ello se muestra el PDR obtenido en promedio por los nodos diferenciando su nivel de egoísmo p_s, y comparando la aplicación de las técnicas centralizadas BC y SC propuestas en los apartados 8.1 y 8.2 (individual y conjuntamente, lo cual se indica en la leyenda con un signo '+'), con la aplicación exclusiva de técnicas de detección local. Como se comentó anteriormente, el PDR es una medida del grado de conectividad conseguido. Al ser representado en función del nivel de egoísmo de los nodos, permitirá apreciar si se consigue aislar a los nodos egoístas (haciendo que tengan un PDR reducido) sin perjudicar a los nodos cooperativos. Se muestran los resultados pertenecientes a los dos escenarios diferentes considerados: en las Figuras 8-11 a 8-14 se representa el escenario I, con menor conectividad, mientras que en las Figuras 8-15 a 8-18 se muestra el escenario II. Al presentar dos escenarios con distinto nivel de conectividad y exposición a nodos egoístas se podrá apreciar el efecto de las técnicas BC y SC propuestas en distintas condiciones. Además, cada una de las figuras corresponde a una técnica de detección diferente para la evaluación del egoísmo de los nodos, como puede leerse en el pie de cada una. De esta manera se podrá comprobar si el diferente

rendimiento de las técnicas bayesianas y exponenciales evaluado en el capítulo 7 repercute o no finalmente en el rendimiento de las técnicas de reputación y de qué manera lo hace, ya sea con un mejor aislamiento de los nodos egoístas o en otros términos[51].

Las figuras de PDR reflejan una circunstancia común: no se consigue aislar a los nodos egoístas empleando únicamente técnicas de reputación locales, sin recurrir a la entidad central. Se aprecia que, en este caso, el nivel de conectividad alcanzado por todos los nodos es similar, independientemente de su grado de egoísmo y de la técnica de detección que se aplique. De hecho, el aspecto de las curvas de PDR en las que únicamente se emplea la detección y el aislamiento local es similar al mostrado en las Figuras 8-9 y 8-10, cuando se aplica únicamente el protocolo de enrutamiento DYMO sin ninguna técnica de reputación adicional. Esto se debe a que, aunque los nodos egoístas son detectados localmente, la información de su identidad no se propaga a otros nodos. De esta manera, los nodos que detectan localmente a algunos nodos egoístas los evitan, pero no consiguen que otros nodos participen en el aislamiento de los nodos egoístas. Se podrá ver posteriormente en los apartados 8.3.7 y 8.3.9 que, de hecho, el número de acusaciones cuando sólo se emplea la detección local es mayor que cuando se emplean técnicas centralizadas, pero son acusaciones locales.

Para corregir este efecto, la técnica BC propaga la información de la identidad de los nodos que son detectados como egoístas a todos los nodos de la red. De esta manera, es posible conseguir un aislamiento correcto de los nodos que son detectados, como muestran las Figuras 8-11 a 8-18, en las cuales el PDR de los nodos egoístas desciende considerablemente, tanto más cuanto mayor es el grado de egoísmo del nodo. Sin embargo, junto con el descenso de la conectividad de los nodos egoístas aparece también un descenso del PDR de los nodos cooperativos. Este efecto indeseable de la técnica BC se debe al hecho ya conocido de que las técnicas de detección utilizadas tienen cierto error, provocadas por el error de detección de *watchdog*, p_e, causado por errores de transmisión radio y colisiones de paquetes. Cuando se utiliza la técnica BC para difundir la identidad de los nodos detectados en toda la red y aislarlos, se difunde también la identidad de los nodos cooperativos que son detectados erróneamente como egoístas, provocando que el PDR promedio de los nodos cooperativos descienda. Esto se comprobará posteriormente al evaluar el porcentaje de acusaciones incorrectas.

Para tratar de evitar las acusaciones incorrectas a nodos cooperativos y por tanto el descenso de su nivel de conectividad, se aplica la técnica SC. Sin embargo, antes de

[51] En las Figuras 8-11 a 8-18 se han utilizado las técnicas de detección BIW, BDF, EFW y EIW para ser comparadas entre sí. El considerar las otras dos técnicas, del total de las seis evaluadas en el capítulo 7, no habría aportado diferencias significativas, por lo que por razones de espacio no han sido consideradas aquí. Por la misma razón, en las siguientes figuras del capítulo, también por razones de espacio se han comparado en algunas de ellas únicamente la técnica BIW como representante de las técnicas bayesianas, y la técnica EIW como representante de las técnicas exponenciales.

comprobar el funcionamiento conjunto de ambas técnicas, se evaluó el de la técnica SC por separado. La técnica SC, al igual que la técnica BC, consigue aislar algunos de los nodos más egoístas: la forma de la curva de PDR en las figuras desciende conforme aumenta el egoísmo. SC consigue incrementar el PDR de los nodos cooperativos respecto a la técnica BC (de manera más acentuada en el escenario II), pero a su vez hay un porcentaje de nodos egoístas, con un grado de egoísmo elevado (p_s>0.5), que con la técnica BC conseguían ser aislados (y su PDR casi nulo) y no lo son con la técnica SC. Esto es porque SC no difunde la identidad de los nodos egoístas, sino que su identidad solamente es conocida por el nodo que desencadena el proceso de SC, de ahí que no se pueda aislar completamente a los nodos más egoístas.

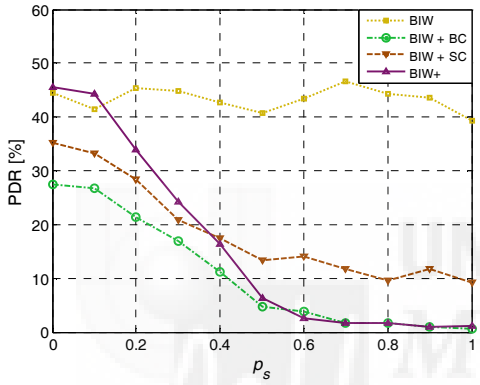


Figura 8-11. PDR de la técnica BIW y técnicas centralizadas BC y SC en escenario I.

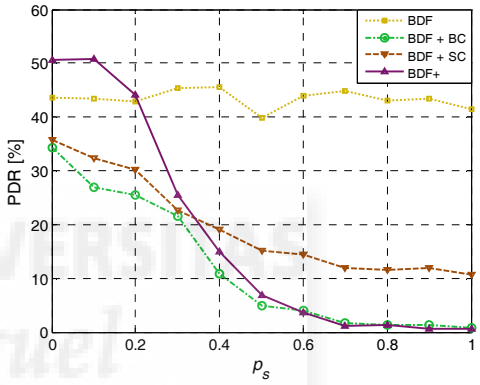


Figura 8-12. PDR de la técnica BDF y técnicas centralizadas BC y SC en escenario I.

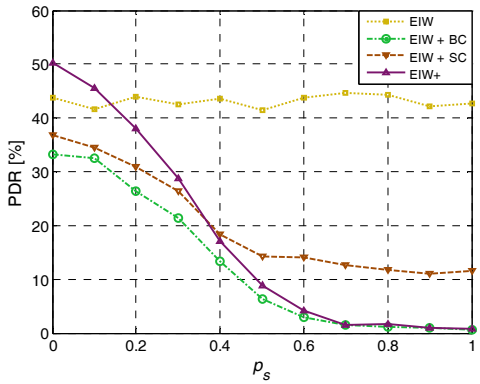


Figura 8-13. PDR de la técnica EIW y técnicas centralizadas BC y SC en escenario I.

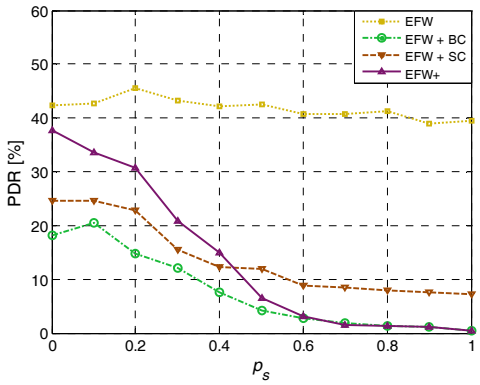


Figura 8-14. PDR de la técnica EFW y técnicas centralizadas BC y SC en escenario I.

La utilización de las dos técnicas conjuntamente reúne las ventajas de ambas: el PDR de los nodos cooperativos se eleva por encima del nivel conseguido al no aplicar ninguna técnica de reputación, o al aplicar únicamente una técnica de reputación con detección local, mientras que se consigue aislar satisfactoriamente a los nodos más egoístas tal y como sucedía en la técnica BC. De hecho, en el escenario I, con una conectividad más restringida por la mayor presencia de egoístas y la menor potencia de transmisión, la aplicación conjunta de BC+SC consigue un nivel de PDR de los nodos cooperativos superior al que se podría obtener aplicando la técnica PD (comparar las Figuras 8-9 y 8-13), en la que la identidad de los nodos egoístas es conocida de antemano. Esto es debido a que cuando se aplican las técnicas BC+SC no todos los nodos con un grado de egoísmo menor (p_s<0.5) son aislados. Aunque esto no es un efecto deseado, puesto que no todos los nodos egoístas son castigados, tampoco es muy perjudicial, dado que los paquetes que descartan estos nodos no es muy alto, su impacto es reducido. En cuanto a la comparación entre las distintas técnicas de detección, puede apreciarse que todas exhiben un comportamiento similar, si bien varía el nivel de conectividad alcanzado por los nodos cooperativos en cada una de ellas al aplicar conjuntamente las técnicas BC+SC. Salvando esta diferencia, las conclusiones sobre el PDR alcanzado al aplicar las distintas técnicas BC y SC tienen la misma aplicación, independientemente de la técnica de detección empleada.

Por último, las Figuras 8-15 a 8-18 muestran los resultados de PDR promedio en el escenario II, en el que la proporción de nodos egoístas menor (20%) y la mayor potencia de transmisión favorecen una mayor conectividad. Efectivamente, las mismas tendencias comentadas anteriormente para el escenario I son aplicables a este escenario: ineficaz aislamiento de los nodos egoístas cuando no hay difusión de las detecciones de nodos egoístas, reducción de PDR de los nodos egoístas con la técnica BC, pero también para los nodos cooperativos, lo cual se soluciona aplicando adicionalmente la técnica SC, que corrige la reducción del PDR de los nodos cooperativos y consigue el máximo nivel de conectividad para ellos, frente a un aislamiento eficaz de los nodos egoístas. La diferencia entre las Figuras 8-15 a 8-18 del escenario II y las Figuras 8-11 a 8-14 del escenario I estriban en que ahora el PDR máximo alcanzable por los nodos cooperativos es mayor. Esto se debe a que la disponibilidad de rutas es más elevada, haciendo que la proporción de paquetes perdidos sin ruta sea menor que en el escenario I (esto se verá en las Figuras 8-19 a 8-22). En este caso, el PDR de los nodos cooperativos al aplicar las técnicas BC y SC conjuntamente en la Figura 8-17 no es mayor que con la técnica PD en la Figura 8-10. La razón es que en este escenario la disponibilidad de rutas es mayor y por tanto se puede alcanzar la máxima conectividad para los nodos cooperativos. Recurrir a la utilización de los nodos con un egoísmo más reducido no contribuye a aumentarla.

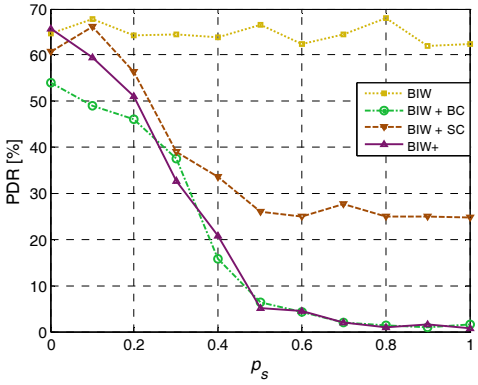


Figura 8-15. PDR de la técnica BIW y técnicas centralizadas BC y SC en escenario II.

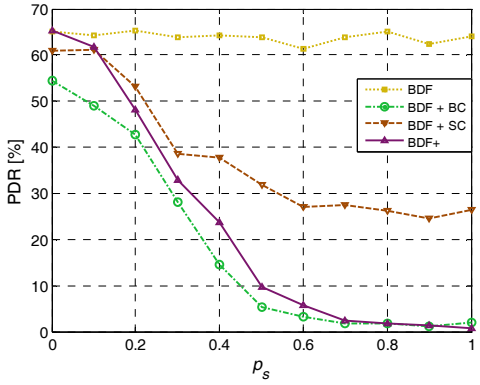


Figura 8-16. PDR de la técnica BDF y técnicas centralizadas BC y SC en escenario II.

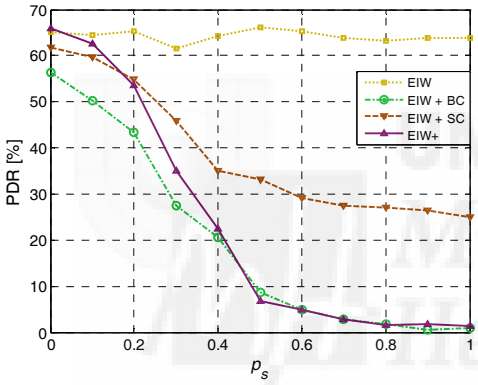


Figura 8-17. PDR de la técnica EIW y técnicas centralizadas BC y SC en escenario II.

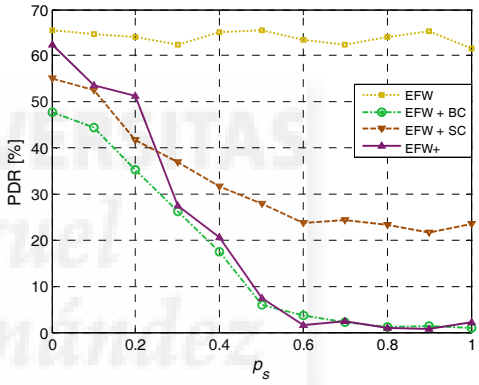


Figura 8-18. PDR de la técnica EFW y técnicas centralizadas BC y SC en escenario II.

La mayor parte de los paquetes que no son entregados al destino (con las técnicas centralizadas BC y SC) está constituida por paquetes que son descartados porque los nodos no encuentran una ruta por la que encaminarlos. Esta circunstancia se refleja en las Figuras 8-19 a 8-22, que muestran el porcentaje de paquetes descartados sin ruta en promedio. Se representan las curvas correspondientes a distintas técnicas: "Sin detección" corresponde a la aplicación del protocolo DYMO sin ningún mecanismo adicional de reputación, "TEAM + WRAM" corresponde a la aplicación conjunta de ambas técnicas, y el resto corresponde a la aplicación de las técnicas de reputación presentadas en este capítulo. "BIW" y "EIW" hacen referencia a la aplicación de estas técnicas de detección de manera local[52], sin recurrir a la entidad central, mientras que las restantes tres etiquetas

[52] Se muestran únicamente estas dos técnicas por claridad, debido a que ofrecen el mejor rendimiento de los enfoques Bayesiano y exponencial respectivamente.

de la leyenda se refieren a la aplicación individual y conjunta de las técnicas centralizadas: BC, SC y su aplicación conjunta: "BIW+" y "EIW+". Además, las Figuras 8-19 y 8-20 representan el escenario I, con una menor conectividad, mientras que el escenario II se ha representado en las Figuras 8-21 y 8-22.

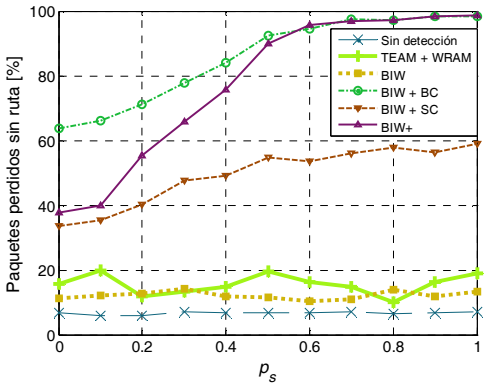


Figura 8-19. % paquetes sin ruta de la técnica BIW y técnicas centralizadas escenario I.

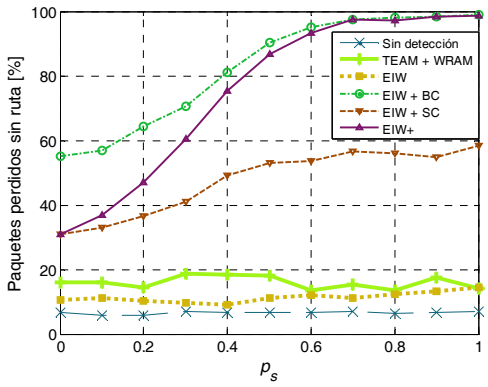


Figura 8-20. % paquetes sin ruta de la técnica EIW y técnicas centralizadas escenario I.

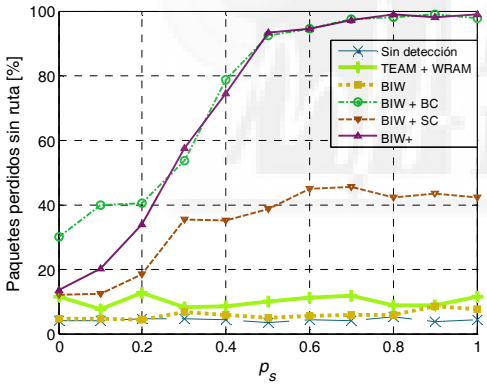


Figura 8-21. % paquetes sin ruta de la técnica BIW y técnicas centralizadas escenario II.

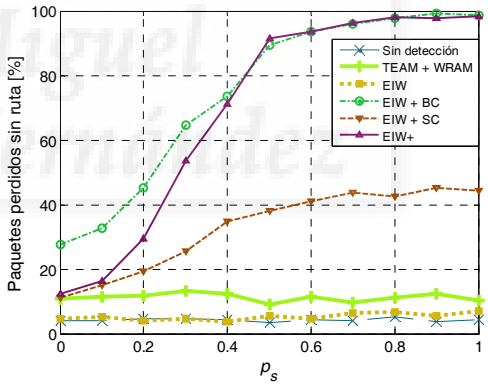


Figura 8-22. % paquetes sin ruta de la técnica EIW y técnicas centralizadas escenario II.

Las Figuras 8-19 a 8-22 muestran claramente que las técnicas que aislan en parte o casi totalmente a los nodos egoístas (las técnicas centralizadas), lo consiguen porque los nodos egoístas no pueden hallar rutas para encaminar sus paquetes. Por el contrario, aplicar cualquier técnica de reputación de manera local tiene un efecto similar al de no aplicar ningún tipo de técnica: el porcentaje de paquetes perdidos sin ruta se sitúa en torno al 10% y se mantiene constante independientemente del grado de egoísmo del nodo origen del paquete. Más concretamente, la técnica BC, que aplicada por separado provocaba un descenso muy acusado del PDR de los nodos cooperativos, como se mostró

en las figuras anteriores, es la técnica con una mayor porcentaje de paquetes descartados sin ruta procedentes de nodos cooperativos. La técnica SC consigue reducir ese porcentaje, pero a su vez también se reduce el aislamiento de los nodos más egoístas y su porcentaje de paquetes descartados sin ruta. Únicamente la aplicación conjunta de las dos técnicas BC y SC consigue que el porcentaje de paquetes sin ruta de los nodos cooperativos sea razonablemente reducido (en función de la conectividad del escenario) mientras que para los nodos más egoístas el porcentaje de sus paquetes que llegan al origen es casi residual (paquetes enviados por ellos antes de que su comportamiento egoísta fuera detectado).

En cuanto a la conectividad en función del escenario de los nodos con distinto grado de egoísmo, comparando las Figuras 8-21 y 8-22 con las Figuras 8-19 y 8-20 puede apreciarse que en el escenario II, con una menor proporción de nodos egoístas y una mayor potencia de transmisión, el número de paquetes que se descartan sin ruta con origen en nodos cooperativos es muy reducido, pero esto no impide que los nodos con mayor grado de egoísmo (p_s>0.5) sí sean aislados. Mientras que para los nodos cooperativos el porcentaje de paquetes descartados sin ruta es menor del 10%, para los nodos con un grado de egoísmo p_s>0.5 asciende a más del 90% en el escenario II. En el escenario I (Figuras 8-19 y 8-20), debido a la mayor presencia de nodos egoístas y a la menor potencia de transmisión, hay un mayor número de paquetes de los nodos cooperativos que son descartados sin ruta. Aún así, la aplicación conjunta de las técnicas BC+SC consigue reducirlo a un nivel entre el 30% y el 40%, según se aplique la técnica de detección exponencial EIW (Figura 8-20) o bayesiana BIW (Figura 8-20).

Las Figuras 8-23 a 8-26 representan el porcentaje de paquetes descartados por nodos egoístas, en función del grado de egoísmo del nodo origen de los paquetes. Como en la métrica de rendimiento anterior, se presentan por separado los distintos escenarios y las dos técnicas de detección analizadas (BIW y EIW, por ser las que obtienen un mejor rendimiento de los enfoques Bayesiano y exponencial). En general, en todos los casos, el porcentaje de paquetes descartados por nodos egoístas no varían respecto al grado de egoísmo del nodo origen. Esto se debe a que los nodos egoístas descartan paquetes independientemente de la identidad del nodo que lo origina. En cuanto a las técnicas, esto se cumple para cuatro de las que se representan: “Sin detección”, TEAM + WRAM, para la técnica bayesiana BIW o exponencial EIW en solitario, y para estas técnicas en combinación con la técnica SC. Sin embargo, se aprecia que al aplicar la técnica BC o las dos técnicas centralizadas conjuntamente (BC+SC), se produce un descenso del porcentaje de paquetes descartados por nodos egoístas conforme aumenta el grado de egoísmo de los nodos origen. La justificación de esto viene de las Figuras 8-19 a 8-22 que representaban el porcentaje de paquetes descartados sin ruta. Debido a que estas técnicas consiguen aislar a los nodos egoístas, los paquetes que son originados por ellos no llegan

a ser descartados por otros nodos egoístas, dado que no se encuentra una ruta por las que puedan ser encaminados.

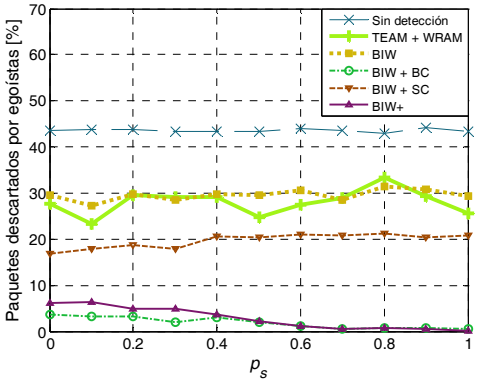


Figura 8-23. % paquetes descartados por nodos egoístas de la técnica BIW y técnicas centralizadas en escenario I.

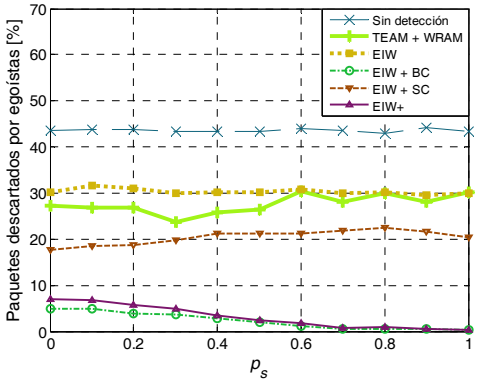


Figura 8-24. % paquetes descartados por nodos egoístas de la técnica EIW y técnicas centralizadas en escenario I.

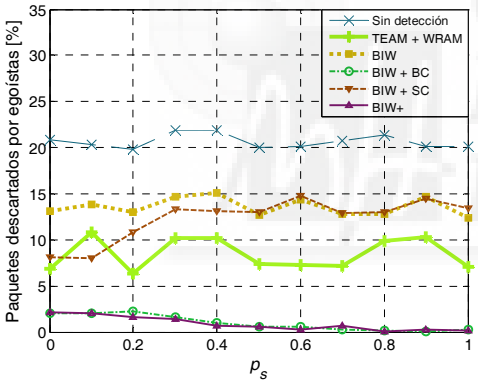


Figura 8-25. % paquetes descartados por nodos egoístas de la técnica BIW y técnicas centralizadas en escenario II.

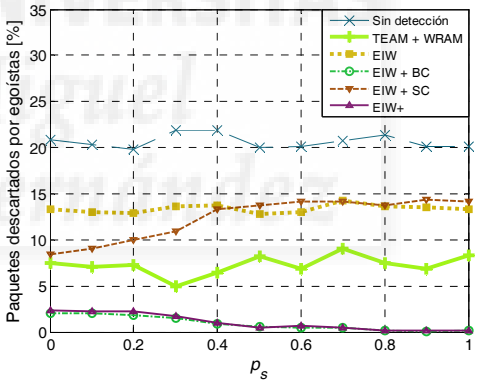


Figura 8-26. % paquetes descartados por nodos egoístas de la técnica EIW y técnicas centralizadas en escenario II.

Por otro lado, en cuanto a los distintos escenarios, sí se aprecian diferencias en esta métrica entre ellos. En el escenario I (Figuras 8-23 y 8-24), con una potencia de transmisión de 17dBm y una proporción mayor de nodos egoístas, el número de paquetes descartados por los nodos egoístas es mayor. La red en este escenario está más expuesta a la acción de los nodos egoístas, debido a que hay una proporción mayor de ellos y además las transmisiones multi-salto necesitan un mayor número de saltos para llegar desde el origen al destino. Además, en el caso de no aplicarse ninguna técnica de reputación ("Sin detección"), la exposición a los nodos egoístas es mayor, siendo más elevado el porcentaje de paquetes que llegan a descartar que con las demás técnicas. Las técnicas

TEAM+WRAM y las de detección local (BIW y EIW) tienen un porcentaje de paquetes descartados por egoístas menor que cuando no se aplica ninguna técnica, debido a que esto es compensado por un mayor porcentaje de paquetes descartados sin ruta (Figuras 8-19 a 8-22) y de paquetes descartados por su origen sospechoso (parámetro que se presenta en la Figura 8-28 y que en el caso de "Sin detección" es nulo).

Las Figuras 8-27 y 8-28 muestran respectivamente el porcentaje de paquetes descartados por caída del enlace y por ser paquetes sospechosos (sólo se representa la técnica de detección BIW porque las conclusiones son similares para el resto). Las técnicas de reputación empleadas descartan aquellos paquetes que estaban esperando a ser retransmitidos cuando detectan que su origen es un nodo egoísta. Estos paquetes son categorizados como paquetes descartados sospechosos en la Figura 8-28. Estos dos parámetros no tienen una gran dependencia respecto a la variación del grado de egoísmo p_s de los nodos origen de los paquetes. Se observa que para las técnicas que más restringen la conectividad de los nodos egoístas (BC y BC+SC), dado que la mayoría de los paquetes con origen en los nodos con mayor grado de egoísmo son descartados sin ruta porque son aislados por los demás nodos, sí se aprecia un descenso del porcentaje de paquetes descartados en ambas figuras (Figuras 8-27 y 8-28).

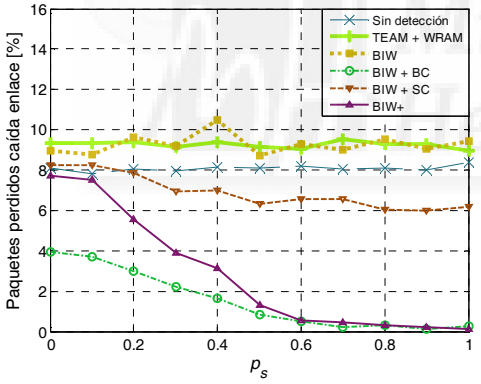


Figura 8-27. % paquetes descartados por caída de enlace de la técnica BIW y técnicas centralizadas en escenario I

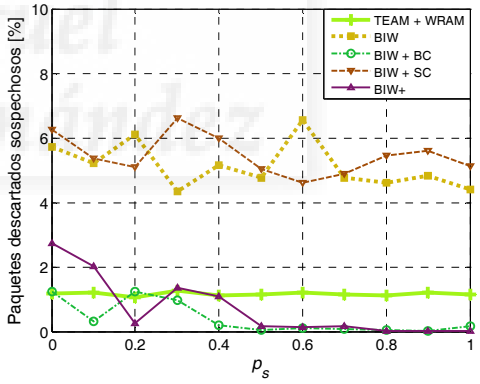


Figura 8-28. % paquetes descartados por origen sospechoso de la técnica BIW y técnicas centralizadas en escenario I

8.3.5 Señalización de técnicas centralizadas

Las Tablas 8-2 y 8-3 muestran el coste en términos de mensajes intercambiados con la entidad central que conlleva utilizar las técnicas presentadas en este capítulo. En la Tabla 8-2 se recogen los resultados referentes a la técnica BC, en concreto, el número total de procesos BC llevados a cabo durante la simulación, entendiendo por este proceso el

descrito en el apartado 8.1. Este proceso implica dos tipos de mensajes en el interfaz celular radio. Primero, el mensaje de alarma enviado desde el nodo precursor que detecta el comportamiento egoísta de otro nodo retransmisor hacia la entidad central. Segundo, el mensaje con la identidad del nodo egoísta, que es difundido desde la entidad central hacia todos los nodos en el área (Figura 8-29).

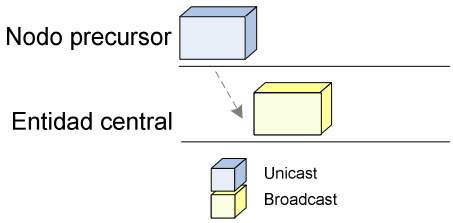


Figura 8-29. Diagrama temporal de mensajes en el proceso BC.

Además, las Tablas 8-2 y 8-3 muestran el número de procesos en los que el nodo sospechoso era en realidad egoísta y en los que el nodo era cooperativo (también en términos porcentuales entre paréntesis). Se presentan los resultados para las dos técnicas de detección con mejor rendimiento de cada enfoque (bayesiana BIW y exponencial EIW) a modo de comparación y para el escenario I (el más restrictivo en términos de conectividad). El número total de mensajes, cuando únicamente se aplica la técnica BC, asciende a 286.13 para la técnica BIW, siendo menor para la técnica EIW (Tabla 8-2). Hay que recordar, que cada uno de los procesos BC llevados a cabo implica la acusación de un nodo. Por ello, del total de 404 nodos (se descuenta el nodo que actúa como entidad central para sumar 405), alrededor de un 70% de los nodos resultan ser acusados. En este contexto, cabe distinguir entre los procesos BC justificados, que llevan a la acusación y el aislamiento de nodos verdaderamente egoístas, y aquellos que provocan el aislamiento de nodos cooperativos. Del total de procesos BC desencadenados, el porcentaje de procesos justificados es alrededor del 64% para la técnica BIW (alrededor del 68% para la técnica EIW). Sin embargo, en ambos casos, el porcentaje de ocasiones en que nodos cooperativos resultan ser aislados es demasiado elevado (mayor del 30%). Esto está en consonancia con los resultados anteriores de PDR (Figuras 8-11 a 8-18), en las que se apreciaba el descenso del PDR obtenido por los nodos cooperativos al aplicar la técnica BC, y con los resultados de paquetes descartados sin rutas (Figuras 8-19 a 8-22).

A la vista del elevado porcentaje de nodos cooperativos que son acusados al aplicar únicamente la técnica BC, y que por tanto son aislados de la red multi-salto celular, se hace necesario evaluar la aplicación conjunta de las técnicas BC+SC. Se puede apreciar de nuevo en la Tabla 8-2 que esta opción proporciona resultados más positivos. En concreto, el número total de mensajes generados se reduce a alrededor de un 50% (del total de nodos en el escenario) para las dos técnicas. Además, con la técnica de detección EIW aplicada junto con las técnicas BC+SC se consigue reducir el porcentaje de procesos

en los que se acusa a nodos cooperativos a tan solo un 11.76% (un 17.72% en el caso de la técnica BIW). Es decir, del total de 191.35 mensajes de acusación, casi un 90% recaen sobre nodos realmente egoístas. Esto se debe a que la técnica SC permite corregir en gran parte las acusaciones incorrectas que se derivarían de la aplicación única de la técnica BC. Además, este resultado también está en consonancia con las Figuras 8-11 a 8-18, en las que al aplicar las técnicas BC+SC los nodos cooperativos obtenían un elevado PDR y un reducido porcentaje de paquetes descartados sin ruta, frente a los nodos con un egoísmo más elevado.

	BC		BC + SC	
	BIW	EIW	BIW	EIW
Total sospechosos (% del total de nodos)	286.13 (70.82%)	262.00 (64.85%)	214.49 (53.09%)	191.35 (47.36%)
Sospechoso egoísta (% del total sospechosos)	183.25 (63.97%)	177.83 (67.87%)	176.51 (82.28%)	168.83 (88.24%)
Sospechoso cooperativo (% del total sospechosos)	102.88 (36.01%)	84.17 (32.13%)	37.98 (17.72%)	22.52 (11.76%)

Tabla 8-2. Sobrecarga por señalización de mensajes de procesos SC

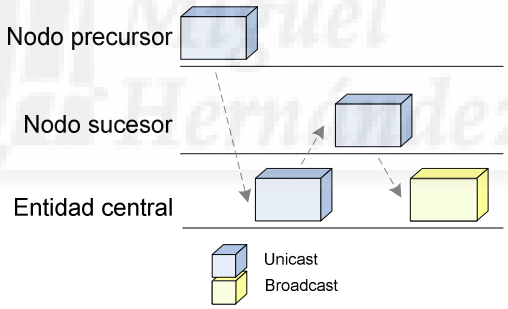


Figura 8-30. Diagrama temporal de mensajes en el proceso BC+SC

La Tabla 8-3 presenta los resultados sobre el número de procesos SC generados durante el tiempo de simulación, aplicando la técnica SC individualmente o bien junto con la técnica BC. Cada proceso de la técnica SC, explicada en el apartado 8.2, implica una secuencia de mensajes transmitidos por el interfaz radio entre los móviles y la entidad central, representados en la Figura 8-30 (aplicadas conjuntamente las técnicas BC+SC). En primer lugar, un mensaje de alarma que inicia el proceso desde el nodo precursor que detecta el comportamiento egoísta de un nodo hacia la entidad central. En segundo lugar hay un intercambio de mensajes entre la entidad central y el nodo sucesor. En el primer mensaje, la entidad central solicita al nodo sucesor información sobre los paquetes recibidos del enlace entre el precursor y el nodo retransmisor, cuyo comportamiento

egoísta se está evaluando. En el segundo mensaje, el nodo sucesor proporciona a la BS la información que había solicitado. Si se aplica la técnica BC también, y el nodo debe ser acusado, su identidad es difundida por la red en un mensaje *broadcast* (Figura 8-30) por la entidad central.

El resultado de un proceso SC puede resultar en una acusación definitiva del nodo o en su no acusación, si la evidencia acumulada en el proceso SC lo justifica. Hay que notar que, en caso de no aplicarse la técnica SC, todas las detecciones locales generadas por los nodos acabarían en acusaciones. Por ello, del total de procesos SC generados, en la Tabla 8-3 se desglosan dos apartados: procesos SC llevados a cabo sobre nodos cooperativos y sobre nodos egoístas. Dentro de la primera categoría, la de nodos cooperativos, caben dos opciones: no acusación (lo que constituye un acierto) o acusación (constituye un error). Igualmente, en la segunda categoría, procesos SC sobre nodos egoístas, caben dos opciones: acusación (acierto) o no acusación (error).

		SC		BC + SC	
		BIW	EIW	BIW	EIW
Número total de procesos SC		3168.51	3058.41	496.51	424.84
Procesos sobre nodos cooperativos	Totales	440.11 13.89%	416.80 13.63%	249.99 50.35%	184.68 43.47%
	No acusación	86.68%	88.99%	84.81%	87.81%
	Acusación	13.32%	11.01%	15.19%	12.19%
Procesos sobre nodos egoístas	Totales	2728.40 86.11%	2641.61 86.37%	246.52 49.65%	240.16 56.53%
	Acusación	75.39%	76.83%	71.60%	70.30%
	No acusación	24.61%	23.17%	28.40%	29.70%

Tabla 8-3. Sobrecarga por señalización de mensajes de procesos BC

El objetivo de las técnicas de detección es que el número total de procesos SC aplicados sobre nodos cooperativos sea mínimo. Considerando la utilización individual de SC, el número total de procesos SC sobre nodos cooperativos es menor para EIW que para BIW (416.80 frente a 440.11). Esto representa un 13% aproximadamente del total de procesos SC. La técnica SC consigue que la mayor parte de los nodos cooperativos implicados (cerca de un 90%) no acaben siendo acusados y aislados. Por otro lado, el total de procesos SC sobre nodos egoístas es el 86% del total de procesos SC desencadenados por las técnicas de detección BIW y EIW. Por tanto, en un porcentaje bastante alto, estas técnicas de detección son efectivas para detectar a nodos egoístas. Sin embargo, la aplicación de SC, si bien permite evitar un porcentaje elevado de acusaciones incorrectas, también produce que algunos nodos egoístas detectados por BIW y EIW no

sean finalmente acusados (alrededor de un 24% del total de procesos de SC desencadenados sobre nodos egoístas).

El número total de procesos SC desencadenados desciende notablemente cuando se combina la utilización de las técnicas BC+SC, de más de 3000 a menos de 500. En términos relativos, se reducen de 1.36 a 0.19 procesos por hora y por nodo. En concreto, utilizando las técnicas BC+SC, la técnica EIW genera menos procesos SC que la técnica BIW (425 frente a 497), menos procesos SC sobre nodos cooperativos (185 frente a 250), y también un número menor de procesos SC sobre nodos cooperativos que acaban en acusaciones incorrectas (12% de 185 frente 15% de 250). Esto se traduce en un número mayor de nodos cooperativos aislados en el caso de BIW, y por tanto, una reducción del PDR promedio de los nodos cooperativos al aplicar conjuntamente las técnicas BC+SC frente al conseguido por la técnica EIW. La utilización de las técnicas BC+SC también hace descender notablemente el número de procesos SC desencadenados contra nodos egoístas y que finalmente son acusados, pero hay que recordar que en este caso se produce un aislamiento total de estos nodos, y por tanto el proceso es mucho más eficiente que cuando se aplica únicamente la técnica SC, lo cual hace que un mismo nodo sea acusado varias veces por nodos distintos.

8.3.6 Capacidad de detección

Las Figuras 8-31 a 8-34 muestran el porcentaje total de nodos que son acusados durante la simulación, en función de su grado de egoísmo. Cada nodo puede ser acusado un cierto número de veces (dado que se muestran distintas técnicas: BIW o EIW sin técnicas centralizadas, BC, SC y su combinación BC+SC), pero en este parámetro se consideran acusaciones únicas, es decir, no se contabiliza el número de veces distintas que ha sido acusado, sino si ha sido alguna vez acusado a lo largo de la simulación. Se muestra a modo de referencia los resultados para la técnica TEAM+WRAM. Se incluyen los resultados para los dos escenarios considerados, con diferente nivel de conectividad.

En general, todas las técnicas coinciden en ser capaces de detectar y acusar a los nodos con un grado de egoísmo p_s>0.5. Las Figuras 8-31 a 8-34 revelan que la técnica TEAM+WRAM, aún habiendo sido diseñada para evitar un excesivo nivel de acusaciones incorrectas, incurre en un excesivo porcentaje de acusaciones a nodos cooperativos (con p_s=0). Si bien este nivel de acusaciones no resulta, como ya se ha visto en las Figuras 8-11 a 8-18 que representan el PDR, un aislamiento real de los nodos acusados, dado que las acusaciones se realizan a nivel local y para que realmente surtieran efecto deberían hacerse de manera global. Otro tanto ocurre con las técnicas de detección BIW y EIW aplicadas en modo local, sin recurrir a las técnicas centralizadas. Superan a la técnica TEAM-WRAM en el sentido en que consiguen rebajar

considerablemente el nivel de acusaciones a nodos cooperativos, si bien todavía oscila en torno al 40%. Este valor, relativamente alto, es debido a que para configurar los parámetros de las técnicas de detección se utiliza un valor de la estimación de p_e constante para ambas técnicas (p_e=0.5), cuando el valor de la p_e real cambia constantemente y toma valores por encima y por debajo de ese valor (ver Figura A-II-9 en el Anexo A-II). Cuando la p_e real toma valores por encima de la p_e=0.5 estimada, se infravalora el valor de p_e y se incurre en mayor riesgo de realizar acusaciones incorrectas (ver Figura 7-15). Por el contrario, cuando p_e toma valores por debajo de 0.5, se sobreestima su valor y se incrementa la tasa de *INA* (Figura 7-16), por lo que hay mayor riesgo de que los nodos con un egoísmo más reducido ($0<p_s<0.5$) no sean acusados.

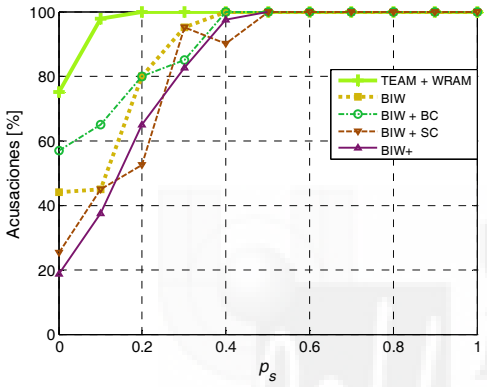


Figura 8-31. % de nodos acusados de técnica BIW y técnicas centralizadas en escenario I

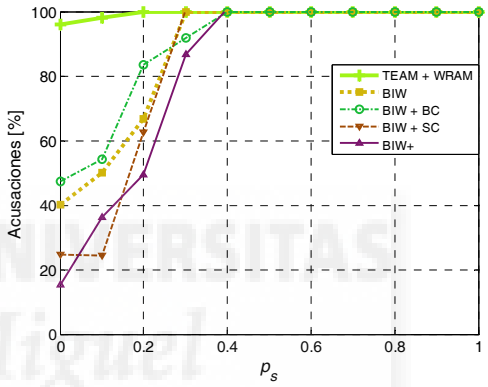


Figura 8-32. % de nodos acusados de técnica BIW y técnicas centralizadas en escenario II

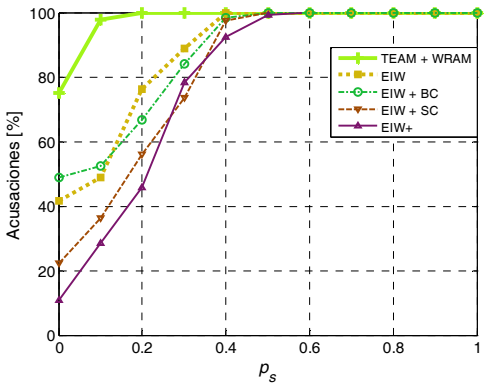


Figura 8-33. % de nodos acusados de técnica EIW y técnicas centralizadas en escenario I

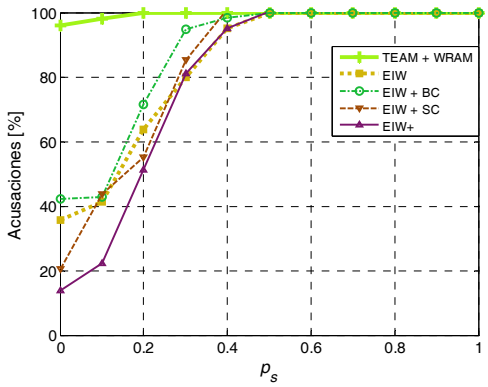


Figura 8-34. % de nodos acusados de técnica EIW y técnicas centralizadas en escenario II

Se aprecia un incremento del porcentaje de acusaciones a nodos cooperativos al aplicar la técnica BC por separado. Esto se debe a que con la técnica BC se incrementa el

número de nodos que son aislados y que por tanto no pueden seguir participando en los procesos de búsqueda de rutas y retransmisión de paquetes. Esto reduce la densidad de nodos cooperativos y la disponibilidad de rutas. Por ello, aumenta también el número de veces que se realizan procesos de búsqueda de rutas y con ello el número de nodos distintos cuyo egoísmo es evaluado y posiblemente detectado. Cuando se detecta localmente el egoísmo de un nodo, dado que no se comprueba con la técnica SC si la detección es correcta, aumentan el número de acusaciones incorrectas. Si se comparan el escenario con menor conectividad (8-31 y 8-33) y el escenario con mayor conectividad (8-32 y 8-34) se observa que al aplicar únicamente la técnica BC, también la menor conectividad y disponibilidad de rutas implica un mayor porcentaje de acusaciones incorrectas a nodos con p_s=0. Una parte importante de las acusaciones incorrectas que resultan en el aislamiento de algunos nodos cooperativos puede solucionarse aplicando la técnica SC. Tanto si se emplea la técnica SC por separado, como conjuntamente con la técnica BC, el resultado es un importante descenso del porcentaje de acusaciones incorrectas, siendo más acusado al emplearlas conjuntamente. Este es en definitiva el objetivo de aplicar la técnica SC, evitar acusaciones incorrectas, sin dejar que los nodos realmente egoístas dejen de ser detectados. De hecho, los nodos en la zona de transición, con un egoísmo $0<p_s<0.5$, ven ligeramente disminuido el porcentaje de acusación al aplicar la técnica SC, aunque a partir de ese nivel de egoísmo, todos los nodos son detectados. La técnica EIW, aplicada junto con las técnicas BC y SC, consigue obtener un porcentaje de acusaciones incorrectas menor que la técnica BIW en ambos escenarios, y por ello los nodos cooperativos obtienen un mayor PDR en las Figuras 8-11 a 8-18.

En el capítulo 7, además de evaluar la precisión de las técnicas de detección, también se evaluaba su velocidad, en términos del número de paquetes δ que son descartados por el nodo egoísta antes de que sea detectado aplicando la métrica correspondiente. Dicho parámetro se representa en las Figuras 8-35 y 8-36, en modo local y con distintas técnicas centralizadas. Los resultados para las técnicas BIW y EIW se representan en las Figuras 8-35 y 8-36. Se observa que las técnicas centralizadas no hacen que la detección de los nodos sea más lenta, respecto a la técnica TEAM+WRAM o respecto a la aplicación de las técnicas BIW y EIW de manera local. De hecho, aunque no queda reflejado en la gráfica, la detección es más eficiente con la técnica BC, dado que a partir de que un nodo egoísta es detectado por primera vez, no tiene que volver a ser detectado por ningún otro, lo cual tendría un coste en términos de paquetes descartados adicionales. No se aprecian grandes diferencias entre las distintas técnicas en las Figuras 8-35 y 8-36. Esto se debe a que el valor del parámetro de configuración l de las técnicas de detección es similar en todas ellas (véase explicación detallada en el Anexo A-II, Tabla A-II-1). Sin embargo, las técnicas bayesianas tienen una mayor imprecisión, como se ha demostrado en las Figuras 8-31 a 8-34 anteriores y en las Tablas 8-2 y 8-3.

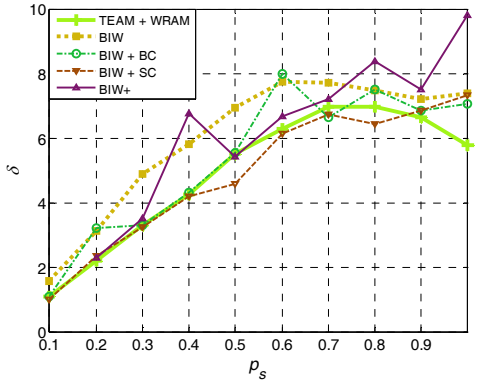


Figura 8-35. Paquetes descartados antes de detección de técnica BIW y de técnicas centralizadas escenario I

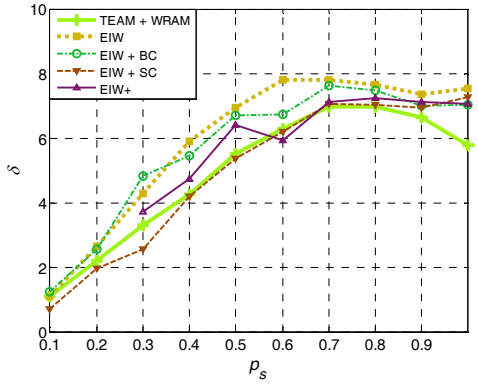


Figura 8-36. Paquetes descartados antes de detección de técnica EIW y de técnicas centralizadas escenario I

8.3.7 Capacidad de reacción

Las técnicas de reputación deben no solo ser capaces de detectar adecuadamente a los nodos egoístas, con los criterios ya conocidos de precisión y rapidez, sino que también deben ser capaces de aislarlos adecuadamente, y de evitar que descarten los paquetes que deben retransmitir. Estos dos últimos aspectos se engloban dentro de la capacidad de reacción de las técnicas de reputación. En cuanto al primero de ellos, el aislamiento de los nodos egoístas, ya fue comentado en el apartado 8.3.6, en las Figuras 8-11 a 8-18 sobre el PDR experimentado por los nodos en función de su grado de egoísmo p_s. Las técnicas centralizadas, especialmente BC y BC+SC, conseguían alcanzar el mayor grado de aislamiento de los nodos egoístas. Por otro lado, el aspecto relacionado con el perjuicio provocado por los nodos egoístas al descartar paquetes, se examina en esta sección.

Las Figuras 8-37 y 8-38 reflejan el perjuicio provocado por los nodos egoístas a la conectividad de la red en función del grado de egoísmo, en términos del número de paquetes descartados en promedio por cada nodo. Sólo se presentan los resultados para el escenario I, puesto que en promedio, los resultados para el escenario II son similares (si se analizaran los totales, en el escenario II el número de paquetes descartados en total sería menor que en el escenario I, por las mejores condiciones de conectividad y la menor proporción de egoístas en la red). En la Figura 8-37 se muestran los resultados de la técnica BIW, en modo local y con las técnicas centralizadas, y en la Figura 8-38 los de la técnica EIW. Además, se incluyen como referencia los resultados obtenidos al no aplicar ninguna técnica de reputación “Sin detección” y al aplicar la técnica “TEAM+WRAM”.

Cuando no se aplica ninguna técnica, el promedio de paquetes descartados por cada nodo es proporcional a su grado de egoísmo. Además, se puede apreciar que a pesar de que el porcentaje de acusaciones únicas (Figuras 8-31 a 8-34) es mayor con la técnica TEAM+WRAM que con las demás, esta técnica es la que resulta en un mayor número de paquetes descartados (Figuras 8-37 y 8-38), descontando el caso en que no se aplica ninguna técnica. La técnica TEAM+WRAM consigue sólo moderar los descartes de paquetes de los nodos más egoístas. La razón de ello es que estos nodos son más fáciles de detectar, y por ello acumulan un número mayor de acusaciones (las Figuras 8-39 y 8-40 muestran el número total de acusaciones registradas a lo largo de la simulación).

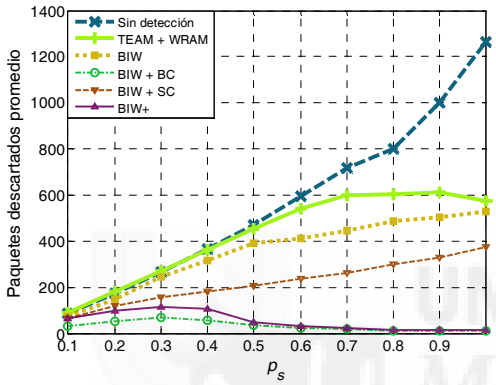


Figura 8-37. Paquetes descartados por nodos egoístas en función del egoísmo del nodo origen, técnica BIW y centralizadas escenario I

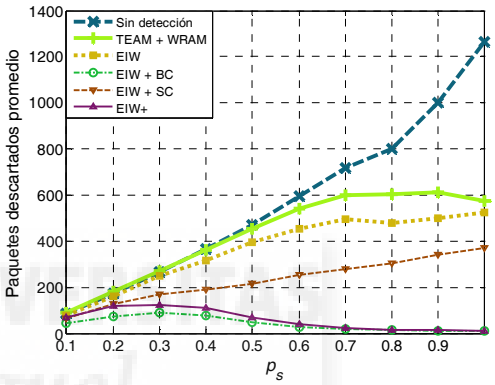


Figura 8-38. Paquetes descartados por nodos egoístas en función del egoísmo del nodo origen, técnica EIW y centralizadas escenario I

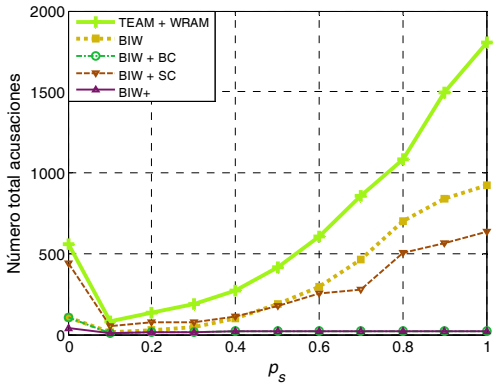


Figura 8-39. Número total acusaciones, técnica BIW y centralizadas, escenario I

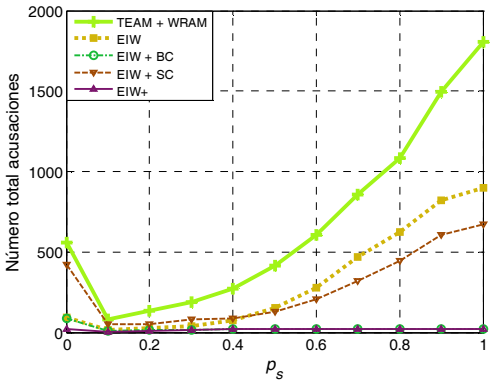


Figura 8-40. Número total acusaciones, técnica EIW y centralizadas, escenario I

Las técnicas BIW y EIW aplicadas de modo local, consiguen disminuir el promedio de paquetes descartados respecto a TEAM+WRAM por la mayor precisión del proceso de

detección. La técnica SC consigue rebajar aún más este parámetro. La razón para ello es que consigue que se realicen menos acusaciones incorrectas (Figura 8-31 y 8-34), y por ello hay una mayor disponibilidad de nodos y rutas seguras. Sin embargo, las únicas técnicas que consiguen realmente evitar el problema de los descartes de paquetes son las técnicas que emplean la difusión de la identidad de los nodos egoístas detectados, BC y BC+SC. La técnica BC lo consigue en mayor grado, por su mayor nivel de acusaciones (Figuras 8-45 a 8-48). Sin embargo, a cambio, la técnica BC aplicada indiviualmente reduce el PDR de los nodos cooperativos (Figuras 8-11 a 8-18), por las acusaciones incorrectas. Además, en las Figuras 8-39 y 8-40, que muestran el número total de acusaciones realizadas, puede observarse que el aislamiento efectivo de los nodos egoístas se realiza con el mínimo número de acusaciones necesario combinando las técnicas BC+SC.

8.4 Conclusiones

A lo largo del trabajo se han presentado y evaluado a fondo diferentes técnicas de reputación, teniendo en cuenta los aspectos más importantes de las mismas. Estas técnicas se componen de dos módulos que interaccionan entre sí para conseguir sus propósitos. Por un lado, el de monitorización, detecta a los nodos que no cooperan en las funciones de la red. Por otro lado, el de reacción tiene una doble función: evitar a los nodos egoístas en las rutas multi-salto para que no descarten los paquetes y aislarlos para que no utilicen la red multi-salto sin contribuir a su mantenimiento y para incentivarlos a cooperar. En el presente capítulo se ha constatado que las técnicas de reputación examinadas hasta ahora tienen un comportamiento deficiente en uno de estos aspectos: el proceso de aislamiento de los nodos egoístas. Si bien consiguen reducir la exposición al egoísmo de los nodos (reducir el número de paquetes que los nodos egoístas descartan), el hecho de que la identidad de un nodo egoísta sólo sea conocida por el entorno del nodo que lo detecta (aislamiento local del nodo) hace que no se consiga un aislamiento efectivo (los nodos egoístas pueden utilizar la red para encaminar sus paquetes sin que a cambio ellos tengan que retransmitir paquetes para otros nodos).

En el presente capítulo se introduce un paradigma de red de comunicaciones cuyas características permiten hacer frente a este problema. Las posibilidades de comunicación y centralización de las redes MCN-MR (Multi-salto *Cellular Network – Mobile Relay*) permiten conseguir una mayor eficacia en el proceso de aislamiento y también una mayor precisión en el proceso de detección. Este capítulo presenta dos técnicas que explotan esta capacidad de la infraestructura de red celular para apoyar los procesos de detección de nodos egoístas y su aislamiento. La primera técnica BC (*Broadcast Category*) tiene como objetivo hacer pública la información local de la identidad de los nodos que son

detectados como egoístas para alcanzar un verdadero aislamiento de los mismos. Por otro lado, debido al error en el proceso de observación de la técnica *watchdog*, es posible que algunos nodos cooperativos sean incorrectamente acusados y aislados injustamente en toda la red. Para evitar esto, se propone de manera complementaria la técnica SC (*Selfishness Check*), que comprueba tras una detección local si realmente un nodo debe ser o no acusado globalmente.

Los resultados obtenidos muestran que no es posible aislar a los nodos egoístas empleando únicamente técnicas de reputación locales como TEAM+WRAM o las técnicas de detección BIW y EIW, sin la asistencia de la entidad central. El nivel de conectividad, en términos de PDR, alcanzado por los nodos es similar, independientemente de su grado de egoísmo, tal y como sucede cuando no se aplica ninguna técnica de reputación (ver Figuras 8-11 a 8-18). Con el aislamiento local realizado en estas técnicas, sin propagar la identidad de los egoístas, únicamente se consigue parcialmente evitar seleccionar a nodos egoístas en las rutas multi-salto, y por tanto se reduce el número de paquetes que los nodos egoístas descartan, pero no se consigue evitar que los egoístas utilicen la red multi-hop para retransmitir sus paquetes. Además, aunque se reduce respecto a no aplicar ninguna técnica de reputación, no se consigue evitar totalmente el descarte de paquetes que los nodos egoístas realizan.

Para conseguir un verdadero aislamiento de los nodos egoístas se necesita la asistencia celular. Con la técnica BC, el PDR de los nodos egoístas desciende considerablemente, tanto más cuanto mayor es el grado de egoísmo del nodo. Sin embargo, junto con el descenso de la conectividad de los nodos egoístas aparece también un descenso del PDR de los nodos cooperativos. Este efecto indeseable de la técnica BC se debe a que las técnicas de detección utilizadas tienen cierto error, inducido por el error de detección de *watchdog*, p_e, causado por errores de transmisión radio y colisiones de paquetes. Con ello, aparte de aislar a los nodos egoístas, BC difunde también la identidad de los nodos cooperativos que son detectados erróneamente como egoístas, provocando que el PDR de los nodos cooperativos descienda. Para tratar de evitar estas acusaciones incorrectas se aplica la técnica SC. Al igual que la técnica BC, SC consigue aislar algunos de los nodos más egoístas al ser utilizada individualmente. Sin embargo, algunos de los nodos más egoístas consiguen evitar el aislamiento. Únicamente la utilización conjunta de ambas técnicas consigue un aislamiento efectivo de los nodos más egoístas y un PDR cercano al máximo (o incluso superior) al alcanzable con la técnica de reputación PD, de los nodos cooperativos, gracias a que con la difusión global de sus identidades, los nodos egoístas no pueden hallar rutas para encaminar sus paquetes. Las Figuras 8-11 a 8-18 muestran el efecto de aplicar las técnicas centralizadas, sobre la conectividad de cada tipo de nodo, según su grado de egoísmo. Las Figuras 8-19 a 8-22 muestran que la mayoría de los nodos egoístas son efectivamente aislados al aplicar conjuntamente las técnicas BC+SC

porque no son capaces de encontrar una ruta para su retransmisión, en comparación con los nodos cooperativos.

La aplicación de las técnicas centralizadas tiene como contrapartida la necesidad de emplear mensajes de señalización entre la entidad central y los nodos. Se ha constatado que el número de mensajes generados por los procesos de difusión de la identidad de los nodos egoístas de la técnica BC genera un número de mensajes que está en todo caso acotado por el número de nodos dentro del sistema. Por otro lado, cuando se aplica la técnica SC individualmente, el número de mensajes no está acotado, pero sí al emplear conjuntamente ambas técnicas. Además, aproximadamente un 90% de los mensajes generados al aplicar conjuntamente ambas técnicas sirven para aislar efectivamente a nodos egoístas. Por último, el número de mensajes generados también depende de las técnicas de detección aplicadas, dado que son las responsables de generar las acusaciones locales que desencadenan los procesos de acusación de las técnicas SC y BC. En este contexto, EIW supera a BIW al necesitar un número menor de mensajes.

9

Conclusiones

En esta tesis han sido empleadas dos tipos de tecnología de redes inalámbricas: redes de comunicaciones móviles celulares y redes MANET. La utilización conjunta de ambas tecnologías genera ventajas y sinergias, como ya ha sido demostrado estudios anteriores. En este contexto, esta tesis ha estudiado la posibilidad de implementación de técnicas de reputación eficaces y eficientes en redes cooperativas con presencia de nodos egoístas, bajo condiciones realistas de funcionamiento. Entre las aportaciones y novedades presentadas, se citan de manera resumida las más destacadas a continuación.

En el capítulo 5 pudo apreciarse el efecto perjudicial que podía tener sobre el rendimiento de las técnicas de reputación y sobre la conectividad de las redes el hecho de considerar modelos realistas de canal y condiciones realistas de simulación, lo cual no había sido suficientemente estudiado en trabajos anteriores. En estas condiciones, era posible apreciar que los errores en la observación del comportamiento de los nodos de la técnica *watchdog* afectaban a la capacidad de las técnicas de reputación para detectar correctamente a los nodos egoístas. Teniendo esto en cuenta, el capítulo 6 investigó diferentes mecanismos que redujeran los efectos perjudiciales sobre la conectividad que provocaban estos errores. Se observó que efectivamente, al aplicar los mecanismos propuestos, se conseguía una importante reducción de las acusaciones incorrectas, lo cual a su vez redundaba en mejorar la conectividad de la red, al estar disponibles un mayor número de nodos y de rutas para la retransmisión de paquetes. En el capítulo 7 se consideró un modelo de nodo egoísta que descarta no todos los paquetes que debe

retransmitir, sino una parte de ellos, escogidos de manera aleatoria. Este tipo de comportamiento hace más difícil el proceso de detección de los nodos egoístas, y plantea un reto considerable en la selección de los valores adecuados para los parámetros de configuración de las técnicas de detección. El capítulo 7 analiza el proceso de detección de nodos egoístas y la configuración de importantes parámetros de las técnicas de detección bayesianas, y propone técnicas de detección exponenciales para facilitar la configuración de las mismas y mejorar la velocidad y la precisión del proceso. Finalmente, el capítulo 8 propone dos técnicas de reputación que, mediante la utilización de la infraestructura de redes celulares, consiguen por un lado detectar adecuadamente a los nodos egoístas, y por otro un aislamiento efectivo de los mismos. Ambos logros contribuyen a mejorar considerablemente la conectividad de los nodos cooperativos. A continuación se detallan las principales conclusiones extraídas de cada uno de los capítulos de resultados.

9.1 Dimensionamiento y viabilidad de sistemas de reputación en redes MANET

El rendimiento de las técnicas de reputación depende en gran medida de la utilización de una técnica de observación fiable, capaz de detectar de manera precisa a los nodos que muestren algún tipo de comportamiento egoísta y también de distinguir los nodos que cooperan adecuadamente en las funciones de mantenimiento de la red. Aunque numerosos trabajos han evaluado anteriormente el rendimiento de distintas técnicas basadas en reputación, hasta la fecha ninguno había empleado modelos de canal y condiciones de simulación realistas, que podrían afectar a la precisión de la técnica de observación, restando fiabilidad a los resultados presentados. Uno de los objetivos del trabajo era comparar ambos enfoques de evaluación de rendimiento aplicados a sistemas de reputación, y mostrar los efectos que pueden tener unas condiciones de simulación demasiado simplistas, para que se puedan corregir las posibles deficiencias de este enfoque en los estudios posteriores.

La técnica de observación más extendida y aceptada entre las técnicas de reputación de la literatura es la técnica de *watchdog*, empleada por primera vez en la técnica de Marti. En la técnica de *watchdog*, cada nodo escucha de manera promiscua las transmisiones que se realizan dentro del rango de cobertura del nodo, para detectar que el nodo correspondiente en la ruta multi-salto realiza correctamente la retransmisión. Para estudiar hasta qué punto podían influir en su rendimiento unas condiciones realistas de simulación, se implementaron dos técnicas de reputación que la utilizaban: la de Marti, tomada como referencia dado que fue la primera en proponer y utilizar el *watchdog*, y la

técnica TEAM, más reciente y que incorpora algunas características avanzadas respecto la técnica de Marti como la reputación recomendada.

Los resultados obtenidos confirmaron la influencia de ciertos parámetros de simulación y dimensionado sobre la eficiencia de las técnicas de reputación. Los factores principales que determinan su rendimiento en presencia de nodos egoístas son la capacidad de detección de la técnica de reputación y el número de saltos promedio de las transmisiones multi-salto. En relación a estos dos factores, se estudiaron una serie de importantes parámetros de simulación que no han recibido suficiente atención en estudios anteriores. El primero y más importante es el modelo de canal radio. Se ha demostrado la conveniencia de emplear un modelo de canal realista frente a los modelos de canal simplificados encontrados en la literatura. La mayoría de los estudios anteriores empleaban un modelo básico de canal radio en el que se establece un rango de transmisión fijo y no refleja las condiciones de transmisión reales. Otro de los modelos de canal radio más extendido, con un grado mayor de realismo pero todavía muy básico, es el modelo de dos rayos, usado por defecto en la plataforma de simulación ns-2. Este es el modelo escogido como umbral inferior de comparación en este estudio, con el que se compararon otros dos modelos de canal que incorporaban efectos realistas tales como las pérdidas de propagación multitrayecto, la correlación espacial del desvanecimiento lento, y las condiciones de visibilidad directa y no directa entre los nodos. Las características más realistas de estos modelos de canal tienen una doble influencia: por un lado aumenta el número de saltos de las transmisiones multi-salto (al disminuir la distancia cubierta en cada salto en promedio), y por otro se aprecia un deterioro de la capacidad de observación de *watchdog* y por tanto también la precisión de las técnicas de reputación, aumentando tanto el porcentaje de acusaciones incorrectas como el porcentaje de falsos positivos. Otros factores de simulación estudiados que también influyen en el rendimiento de las técnicas, especialmente al variar el número de saltos promedio de las transmisiones, son la potencia de transmisión, la densidad de nodos y el tamaño del escenario. También se encontró que la carga de tráfico en el canal inalámbrico influye notablemente en la capacidad de detección de las técnicas de reputación. A la vista de los resultados obtenidos, el objetivo planteado a continuación fue el de tratar de mejorar el rendimiento de las técnicas de reputación evaluadas en condiciones realistas de funcionamiento y simulación.

9.2 Técnicas de reputación distribuidas

Como se comentaba en el apartado anterior, las técnicas de reputación Marti y TEAM sufrían un importante deterioro de su rendimiento al ser evaluadas en condiciones realistas de simulación. Este deterioro era similar en ambas, y en parte provenía del error

en el proceso de observación de la retransmisión de los paquetes al que está sujeta la técnica *watchdog*, provocado por errores de propagación radio y colisiones de paquetes que impiden que el nodo observador escuche correctamente la retransmisión. Debido al error en las observaciones de *watchdog*, algunos nodos cooperativos son acusados erróneamente y potenciales rutas seguras son descartadas. Esto limitaba la capacidad de los nodos de encontrar rutas seguras para encaminar los propios paquetes, ya sea porque eran acusados injustamente o porque acusaban injustamente a otros nodos. Por ello el siguiente paso fue encontrar estrategias que compensasen la inexactitud de *watchdog*, y rebajaran el nivel de acusaciones incorrectas para mejorar la conectividad de las redes MANET.

Se han propuesto tres mecanismos que, al ser aplicados en paralelo a las técnicas de reputación utilizadas como referencia (Marti y TEAM), consiguen el mencionado objetivo desde enfoques diferentes. RAM incentiva de manera más acentuada las retransmisiones observadas correctamente, que sirven para confirmar las retransmisiones que estén pendientes de ser observadas y para restaurar la reputación del nodo que haya podido ser degradada injustamente. RFM combate la disminución de reputación que pueden provocar las caídas del enlace por la naturaleza intrinsecamente variable del canal radio o por la movilidad. Por último, WM introduce una categoría intermedia entre la de nodo cooperativo y nodo sospechoso, que proporciona una oportunidad más al nodo para distinguir las acusaciones correctas a nodos egoístas de las acusaciones incorrectas a nodos cooperativos provocadas por la inexactitud de *watchdog*.

Los resultados obtenidos demuestran que las técnicas propuestas reducen el número de acusaciones incorrectas, e incrementan la disponibilidad de rutas multi-salto seguras. Ambos factores redundan en el incremento del PDR percibido por los nodos. Por otro lado, los resultados muestran un efecto no deseado desencadenado por las técnicas presentadas. A la par que se reducen el número de acusaciones incorrectas, también se reduce, aunque en menor medida, el número de acusaciones correctas, lo cual podría restar capacidad de detección a las técnicas e incrementar el número de paquetes descartados por los nodos egoístas. Sin embargo, los resultados obtenidos demuestran que este efecto no es apreciable sobre el PDR en la mayoría de los casos. En definitiva, la conectividad siempre mejora dado que prevalece el efecto de la mayor disponibilidad de rutas seguras.

A lo largo del trabajo se ha demostrado que el funcionamiento anómalo del *watchdog* provenía tanto de errores en el canal de transmisión como de colisiones de paquetes. Por ello se ha analizado el funcionamiento de las técnicas cuando variaban estos factores. Se modificó la probabilidad de error de transmisión modulando la potencia de transmisión y se comprobó que aumentar el error produce un nivel mayor de acusaciones incorrectas y por tanto una menor disponibilidad de rutas, así como un PDR más reducido. Este efecto

era compensado por las técnicas propuestas. También se modificó la probabilidad de colisiones de paquetes aumentando el porcentaje de sesiones activas de usuario. Al incrementarse las colisiones, se produce un número mayor de acusaciones incorrectas y la disponibilidad de rutas es menor. También en este escenario más adverso, las técnicas propuestas consiguen mejorar el PDR respecto a las técnicas de reputación tradicionales.

9.3 Detección Bayesiana y exponencial

A partir de la evaluación del rendimiento de distintas técnicas basadas en reputación que empleaban como método de observación la técnica *watchdog* se comprobó que las condiciones de simulación y el modelo de canal radio tienen una notable influencia en la probabilidad de error de *watchdog*, es decir, en la probablidad de que *watchdog* tome una acción cooperativa como una acción egoísta. Esta incertidumbre en el proceso de observación dificulta considerablemente el funcionamiento de las técnicas de reputación, al aumentar el número de acusaciones incorrectas, y paralelamente disminuir el número de rutas multi-salto disponibles. En el capítulo 6 se propusieron técnicas que conseguían mejorar la conectividad de la red al contrarrestar los efectos del error de *watchdog* sobre el número de acusaciones incorrectas. Sin embargo, a partir del capítulo 7 se asumió un modelo más general de nodo egoísta, en el cual la acción de descartar un paquete que debe retransmitir sigue una variable aleatoria binomial con cierta probabilidad, la probabilidad de egoísmo. Con esta generalización la detección de los nodos es más complicada, dado que el comportamiento egoísta del nodo puede estar enmascarado por la probabilidad de error de *watchdog*. Las técnicas de reputación suelen usar distintas técnicas de detección para tomar la decisión de acusar o no a un nodo a través de las observaciones del *watchdog*. Este proceso puede requerir realizar una gran cantidad de observaciones para alcanzar una precisión razonable. Un estudio analítico de una técnica de detección tradicional bayesiana como caso paradigmático demostró claramente el compromiso entre la velocidad de detección y la precisión de las decisiones. También aparecen tendencias contrapuestas al tratar de seleccionar los valores óptimos de los parámetros de configuración de las técnicas de detección, que son principalmente el umbral de acusación τ y el número mínimo de observaciones antes de tomar una decisión, l. El valor de τ plantea un compromiso entre la tasa de acusaciones incorrectas y la tasa de no acusaciones incorrectas, mientras que incrementar l puede aumentar la precisión del proceso de detección pero también lo hace más lento. Además, en la selección de los valores óptimos para un determinado escenario deben tenerse en cuenta factores específicos del escenario como la distribución del egoísmo entre los nodos (cuántos nodos egoístas hay, y cuál es su grado de egoísmo) y la distribución de probabilidad del parámetro que mide la probabilidad de error de la técnica de observación *watchdog*.

Para facilitar la selección de los valores de configuración de las técnicas de detección y reducir el compromiso entre velocidad y precisión de la detección, se propuso una técnica de detección con un enfoque alternativo al de las técnicas Bayesianas basada en la función exponencial. La principal novedad de esta técnica era que la probabilidad de error de *watchdog* era considerada explícitamente. Como se vio en los resultados, esto facilitaba la selección de los parámetros de configuración. Para comparar el rendimiento de las técnicas Bayesianas y exponenciales, se llevó a cabo un extenso lote de simulaciones para el cual fue necesario inicialmente determinar los escenarios de simulación en los que se tenían en cuenta aquellos parámetros que más podían influir en la selección de los parámetros de configuración. Estos parámetros eran: la probabilidad de error de *watchdog*, la proporción de nodos egoístas y la distribución del parámetro de egoísmo entre ellos, y el número de observaciones. A partir de las simulaciones se obtuvieron los valores óptimos de configuración de cada una de las técnicas analizadas. Este análisis demostró que una sola configuración de l y τ resultaba ser óptima en las técnicas de detección exponenciales, y que no necesitaba modificarse para ajustarse a las variaciones del parámetro p_e en los distintos escenarios propuestos, mientras que en el caso de las técnicas Bayesianas, los valores de los parámetros de configuración debían reajustarse a cada valor de p_e. Los resultados presentados demostraron que las técnicas exponenciales obtenían el mejor rendimiento en términos de precisión, especialmente para la tasa de no acusaciones incorrectas, con un menor coste en paquetes descartados, es decir, con una rapidez mayor. También se investigó la sensibilidad al error en la estimación de la probabilidad de error. En concreto el estudio realizado demostró que es preferible hacer una sobrestimación del valor del parámetro de probabilidad de error de *watchdog*, para evitar un aumento indeseable de la tasa de acusaciones incorrectas, aunque con ello se tenga que incurrir por otro lado en pequeños incrementos tanto de la tasa de no acusaciones incorrectas como del número de paquetes descartados antes de la detección.

9.4 Técnicas de reputación en redes multi-salto celular

El capítulo 8 introduce un paradigma de red de comunicaciones inalámbrica cuyas características permiten elevar considerablemente el rendimiento de las técnicas de reputación: las redes MCN-MR (Multi-salto *Cellular Network – Mobile Relay*). Las características complementarias de las redes celulares y las redes MANET permiten conseguir una mayor precisión en el proceso de detección y sobre todo, una mayor eficacia en el proceso de aislamiento de los nodos egoístas detectados. Para ello son necesarias también técnicas de reputación diseñadas específicamente para aprovechar el potencial de estas redes. Con ellas se pretende superar los problemas detectados durante

la tesis: el rendimiento anómalo de la técnica *watchdog* cuando las técnicas de reputación eran evaluadas en condiciones de simulación y funcionamiento realistas, y las consecuencias de esto sobre el rendimiento de las técnicas de reputación, que se hacen evidentes en el incremento del número de acusaciones incorrectas, la disminución injustificada del número de rutas disponibles para la transmisión multi-salto, y el descenso de la conectividad de los nodos en términos de PDR. Además de este problema aparece otro, que es que todas las técnicas de reputación evaluadas son ineficaces en el proceso de aislamiento de los nodos egoístas. A pesar de detectar con mayor o menor rapidez y precisión a los nodos egoístas, no consiguen aislarlos a nivel global, debido a que la información de la identidad de los nodos egoístas no se propaga a toda la red, sino que se reduce al ámbito local de los nodos que detectan al nodo egoísta y a algunos nodos vecinos.

Frente a ello, en el capítulo 8 se presentaron dos técnicas que explotan la capacidad de la infraestructura de red celular para apoyar los procesos de detección de nodos egoístas y su aislamiento, tratando de minimizar el coste en términos de mensajes de señalización en el interfaz radio celular. La primera técnica BC (*Broadcast Category*) tiene como objetivo hacer pública la información local de la identidad de los nodos que son detectados como egoístas. Con ello se consigue un verdadero aislamiento global de los nodos que son detectados. Por otro lado, debido al error en el proceso de observación de la técnica *watchdog*, es posible que algunos nodos cooperativos sean incorrectamente acusados y aislados injustamente en toda la red. Para evitar esto, se propone de manera complementaria la técnica SC (*Selfishness Check*), que comprueba tras una detección local si realmente un nodo debe ser o no acusado globalmente.

Los resultados obtenidos muestran que no es posible aislar a los nodos egoístas empleando únicamente técnicas de reputación locales como TEAM+WRAM sin recurrir a la ayuda de la entidad central. El nivel de conectividad alcanzado por los nodos es similar independientemente de su grado de egoísmo, tal y como sucede cuando no se aplica ninguna técnica de reputación, cuando el objetivo debería ser penalizar a los nodos con un mayor grado de egoísmo y mantener o incrementar la conectividad de los nodos cooperativos. Con el aislamiento local realizado de estas técnicas, solo se consigue evitar (parcialmente) a los nodos egoístas en las rutas multi-salto, reduciendo el número de paquetes que los nodos egoístas descartan, pero no se evita que los egoístas utilicen la red multi-salto para retransmitir sus paquetes. Así, los nodos egoístas no tienen ningún incentivo para cooperar, sino que es preferible para ellos usar la red sin prestar sus recursos a cambio. Con la técnica BC, el PDR de los nodos egoístas desciende considerablemente, tanto más cuanto mayor es el grado de egoísmo del nodo. Sin embargo, aparece también un descenso indeseable del PDR de los nodos cooperativos que se debe al error de detección de la técnica de observación *watchdog* que provoca

acusaciones incorrectas difundidas también por la técnica BC. Con la utilización conjunta de las técnicas BC y SC se consigue un PDR cercano al máximo de los nodos cooperativos y un aislamiento efectivo de los nodos más egoístas, dado que la técnica SC consigue corregir en gran parte las acusaciones incorrectas provocadas por el *watchdog*.

La aplicación de las técnicas centralizadas tiene como contrapartida la necesidad de emplear mensajes de señalización entre la entidad central y los nodos. Sin embargo, se ha demostrado que la aplicación conjunta de ambas técnicas no genera un número excesivo de paquetes de señalización, incluso en simulaciones de larga duración. Además, un 90% de los mensajes generados sirven para aislar a nodos egoístas. Por último, el número de mensajes generados al aplicar las técnicas de detección exponenciales propuestas en el capítulo 7 es menor que al aplicar las técnicas de detección bayesianas. También es conveniente mencionar que la adaptación e implementación de las técnicas de detección exponenciales en un escenario realista como el de la simulación fue más sencillo debido a que consideran explícitamente el valor de la probabilidad de error de *watchdog*. También se estudió la influencia del grado de conectividad del escenario variando el nivel de potencia de transmisión y la proporción de nodos egoístas. En el escenario con un menor nivel de conectividad (menor potencia de transmisión y mayor proporción de nodos egoístas) se detecta un mayor porcentaje de paquetes descartados por los nodos egoístas o descartados al no encontrarse una ruta por la cual encaminarlos. Esto, en definitiva, provoca una reducción del PDR de los nodos cooperativos.

9.5 Líneas futuras de investigación

Esta tesis ha demostrado la efectividad de la utilización de las redes celulares como una herramienta poderosa para hacer frente a los desafíos planteados al aplicar técnicas de reputación tradicionales a las redes MANET puras. Entre estos desafíos se encuentra el conseguir un aislamiento efectivo de los nodos más egoístas. La capacidad de la red celular para difundir la identidad de los nodos egoístas entre los nodos de la red resulta esencial para alcanzar un verdadero aislamiento. Sin embargo, sigue existiendo, aunque en menor medida gracias a la técnica SC, la problemática de las acusaciones incorrectas, que al aplicarse un aislamiento global, resulta aún más perjudicial para los nodos. Uno de los objetivos prioritarios surgidos a partir de este estudio sería el de reducir aún más la tasa de acusaciones incorrectas para evitar que los nodos cooperativos sean acusados, con nuevas técnicas o afinando las técnicas ya propuestas. Por otro lado, sería también aconsejable el estudio de políticas de reinserción que permitieran a los nodos egoístas arrepentidos volver a participar en la red como nodos cooperativos. Esto en parte ya se ha sugerido en algunos estudios en los que la cooperatividad o el egoísmo del nodo era un valor "negociable" sobre el que varios nodos en la red se ponen de acuerdo [35]. Sería

interesante ver qué papel mediador puede ofrecer la red actuando en las negociaciones de los nodos con la misión alcanzar un equilibrio de cooperación suficiente para mantener la red y reducir problemas como la interferencia de las transmisiones ad-hoc.

Como se comentó en el capítulo 2, en la literatura sobre egoísmo en MANETs, numerosos estudios se han ocupado de diferentes comportamientos anómalos de los nodos en cuanto a su grado de cooperación en distintas tareas. Esta tesis se ha centrado en el comportamiento egoísta clásico en el que algunos nodos participan en las tareas de enrutamiento, pero por distintas causas no retransmiten todos los paquetes que se les encomienda retransmitir. Una posible ampliación de la tesis podría explorar soluciones en redes multi-salto celulares para hacer frente a otros comportamientos anómalos planteados en la literatura. En esta tesis se ha empleado un modelo de nodo egoísta clásico bastante genérico, en el que el nodo no descarta todos los paquetes sino una fracción de ellos en forma aleatoria, regulado por el parámetro p_s. Se podría ir más allá haciendo que el parámetro p_s no fuera constante sino variable, dependiendo de otros parámetros como la batería del nodo, la predisposición del usuario a cooperar en la retransmisión para otros usuarios, etc.

Esta tesis se ha ocupado exclusivamente de técnicas de reputación que utilizaban la técnica de observación *watchdog* para la vigilancia del comportamiento de los nodos egoístas. Como se comentó en el capítulo 2, hay estudios que han propuesto métodos de observación alternativos. Además, otros comportamientos anómalos distintos del comportamiento egoísta considerado aquí podrían ser también objeto de estudio. En cualquier caso, la exploración de otros tipos de técnicas de observación alternativos al *watchdog*, y su integración en las técnicas de reputación centralizadas, sería otra posible línea a seguir, si bien el modelo de probabilidad de error de la técnica de observación propuesto en el capítulo 7 es bastante general para poder aplicarse a otras técnicas distintas del *watchdog*.

En el capítulo 8 se demostró que para que las técnicas de reputación centralizadas propuestas obtuvieran su mejor rendimiento era necesario que las técnicas de detección que utilizaban pudieran contar con el valor más exacto posible de la probabilidad de error del *watchdog*. En caso de que no fuera posible, era preferible sobreestimar la probabilidad de error para evitar un incremento inaceptable de las acusaciones incorrectas. Sin embargo, reducir más las acusaciones incorrectas sin por ello incrementar excesivamente el número de nodos egoístas no detectados podría conseguirse con un mecanismo más exacto para la estimación de la probabilidad de error. En el capítulo 8 se apuntaba un mecanismo adaptativo para la estimación de la probabilidad de error que se servía de la comunicación con la entidad celular central durante el proceso de SC. Sin embargo, su rendimiento no ha sido el esperado, como muestra el Anexo A-II, y por ello otra posible

línea futura sería corregir el funcionamiento de esta técnica, además de proponer otras o incluso implementar técnicas de estimación de probabilidad de error de la literatura.

A pesar de que en la tesis se han utilizado escenarios y condiciones con un alto grado de realismo, sobre todo en los aspectos más relacionados con la simulación radio, otros aspectos de mayor nivel se han obviado. Podrían estudiarse condiciones más realistas de las redes celulares convencionales tales como la presencia de múltiples operadores, la existencia de múltiples celdas y en distintos niveles de coexistencia (macro, micro, pico, etc.) ¿Qué información sobre los nodos egoístas debería pasar de unas celdas a otras? ¿O es suficiente con aislarlos dentro de una celda, ya que aislarlos en todas las celdas sería un castigo excesivo?

Otro de los temas recurrentes en la literatura sobre MANETs es el de los nodos que van más allá del egoísmo y se comportan maliciosamente para provocar daños en la red intencionadamente. También se han estudiado situaciones en las que los nodos maliciosos colaboran en la red para aumentar el efecto de estos ataques maliciosos. Se abre por tanto una vía para estudiar este tipo de comportamientos y las soluciones posibles dentro del paradigma de las redes multi-salto celular.

Un aspecto fundamental que debe considerarse en trabajos de investigación sobre MANETs son los diferentes tipos de protocolos de enrutamiento. Existe una gran variedad de protocolos de enrutamiento, si bien AODV goza de gran popularidad y aceptación y como se ha comentado, la parte reactiva del protocolo de enrutamiento del estándar de redes mesh 802.11s está basada en este protocolo y en su sucesor DYMO. Es por ello que este trabajo ha considerado exclusivamente el protocolo DYMO. Una posible continuación de este trabajo podría tratar de adaptar las técnicas propuestas a otros protocolos de enrutamiento y evaluar como afectaría este cambio a su rendimiento. También sería interesante la integración de las técnicas de reputación centralizadas propuestas con técnicas de enrutamiento pensadas específicamente para redes MCN, en las que la posibilidad de disponer de la asistencia de una entidad central puede ser de gran ayuda a la hora de optimizar el rendimiento global de la red mediante la selección de las rutas con criterios que no buscan meramente el camino más corto, sino que tienen en cuenta otras métricas como la ausencia de nodos egoístas, entre otros.

Una posible vía de investigación poco convencional, pero con una mayor presencia cada día en la vida cotidiana, podría ser explotar el poder de las redes sociales. En las redes sociales cada usuario establece distintos niveles de privacidad para compartir con sus amigos y conocidos datos personales tales como estados, fotografías, aficiones y enlaces. Otro de los recursos que podrían ser compartidos serían los recursos de comunicación del dispositivo móvil del usuario. En concreto, como si se tratara de un aspecto más a compartir por el usuario, podría especificar cuál sería su política

cooperación en cuanto a participación en redes MCN, teniendo en cuenta aspectos como la batería del terminal, grado de relación con los demás usuarios (amistades, conocidos, desconocidos, pertenencia a una misma institución, etc.)

Finalmente, otra vía que no ha sido explorada es relacionar la decisión de cooperación del nodo o del usuario con la difusión social de la innovación. [141] extrae algunos de los principios utilizados en el estudio de la difusión de la innovación, en áreas como la Economía o la Psicología, y los aplica a investigar cómo los nodos de una red MANET toman decisiones conjuntas, pero de manera distribuida, en cuanto al valor más adecuado de ciertos parámetros de configuración de protocolos, en función de las condiciones del entorno percibidas por cada uno de ellos. En el caso de la cooperación en redes MCN, deberían investigarse cuáles son las condiciones de la red y de los usuarios en las que la elección de la cooperación sería la más adecuada, y cómo pueden los usuarios tomar la decisión conjunta de cooperar o no cooperar en el mantenimiento de la red y el establecimiento de rutas.

UNIVERSITAS
Miguel
Hernández

A-I

Interfaz radio celular en la herramienta ns-2

A pesar de que la implementación del simulador y las adaptaciones y modificaciones necesarias para simular redes MANET ya fueron descritas en el capítulo 4, en este anexo se recogen algunas indicaciones adicionales que se refieren a la implementación de la parte del interfaz radio celular llevada a cabo expresamente para adecuar la herramienta de simulación de redes ns-2 a las necesidades del capítulo 8. Dado que estas necesidades no habían aparecido en otros capítulos, las indicaciones específicas de las redes celulares se recogen en este apartado y no en el capítulo 4.

En una red MCN, existen diversas cuestiones referentes al enrutamiento de los paquetes que deben ser todavía investigadas. La hibridación de la red MANET con la red celular plantea la necesidad de especificar cómo se hallarán las rutas que tengan origen o destino en la entidad central. Esto es especialmente relevante en un posible escenario, que será el considerado en este trabajo en el capítulo 8, en el que la red celular actúa como *backhaul* de los nodos de la red MCN. En dicho escenario, los nodos que quieren acceder a servicios de datos se conectarían a la red bien directamente por el interfaz celular (enlace de datos celular tradicional) o bien a través de la red multi-salto implícita en la red MCN, utilizando como retransmisores a otros nodos hasta llegar a un nodo que acceda a la red celular (comunicación multi-salto celular). En cualquiera de los dos casos,

ilustrados en la Figura A-I-1, es necesario determinar qué criterio seguirán los nodos a la hora de decidir entre acceder directamente a la red celular o bien seguir buscando otros nodos a través de los que enrutar los paquetes, hasta alcanzar un nodo para el cual la calidad del enlace celular sea mayor y por tanto mejore la calidad de la conexión de extremo a extremo. En la Figura A-I-1 se muestra un ejemplo de red MCN. Los nodos ad-hoc son aquellos que participan en la parte ad-hoc de la red, mientras que los nodos híbridos hacen de pasarela hacia la red celular. Los papeles de nodo híbrido y nodo ad-hoc pueden variar en función de las capacidades y las necesidades de cada nodo y del funcionamiento de los protocolos de enrutamiento. De los dos nodos *Destino* que aparecen en la Figura A-I-1, uno de ellos decide utilizar el enlace celular de larga distancia con la estación base para realizar la comunicación, mientras que el otro utiliza la red multi-salto.

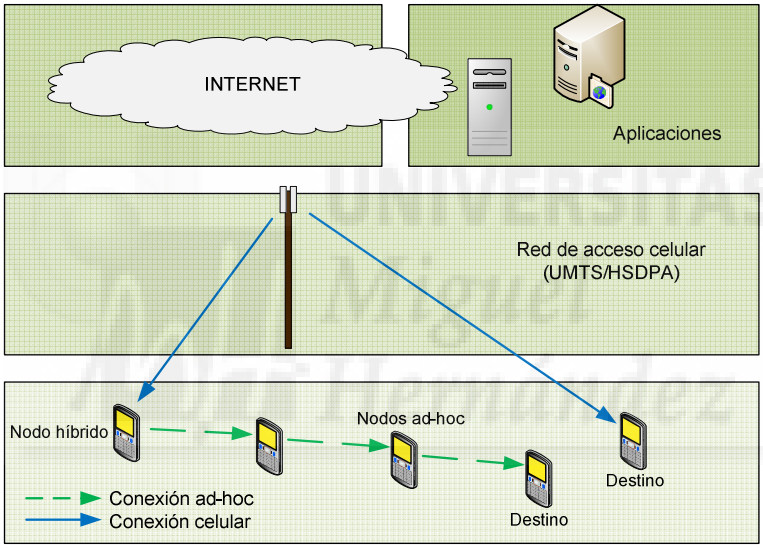


Figura A-1-1. Diagrama de nodos híbridos y nodos ad-hoc en una red MCN.

Dado que el enrutamiento óptimo de los paquetes en una red MCN para la optimización del rendimiento global de la red no es el objeto principal de estudio de esta tesis, se ha optado por establecer un criterio sencillo que permita a los nodos decidir la cuestión de acceder directamente a la red celular o bien participar en la búsqueda de rutas en la parte multi-salto de la red, que se explica a continuación. En una red multi-salto, los nodos utilizan protocolos de enrutamiento para establecer las rutas por donde encaminar los paquetes. En el presente trabajo se ha empleado como protocolo de enrutamiento el DYMO. Dicho protocolo establece que el establecimiento de ruta se inicia con la difusión de un paquete de búsqueda de ruta por parte del nodo origen, que se va retransmitiendo hasta alcanzar al nodo destino. Esta retransmisión la realiza cada nodo que recibe una copia del paquete de búsqueda de ruta, de manera que los paquetes se difunden en modo

broadcast por la red, con ciertas restricciones para evitar transmisiones redundantes o superfluas, y la inundación de la red con mensajes de control. En el caso de que el destino de la transmisión sea la propia entidad central, cada nodo que recibe un paquete de búsqueda de ruta debe evaluar, antes de retransmitirlo, si cumple el criterio requisito para actuar como nodo híbrido. Un criterio sencillo para establecer el nodo híbrido es atendiendo a la calidad del enlace radio celular esperable. Por ello, en el presente trabajo se ha escogido un criterio relacionado con la calidad del enlace radio, basado en las especificaciones del interfaz radio del sistema HSDPA.

HSDPA requiere información de realimentación de la capa física en el enlace ascendente desde el terminal hacia la estación base para permitir el funcionamiento de la funcionalidad de LA (*Link Adaptation*) y de las retransmisiones a nivel de capa física [56]. Esta información se transporta en el canal HS-DPCCH (*High-Speed-Dedicated Physical Control Channel*). El mecanismo de HARQ (*Hybrid Automatic Repeat ReQuest*) informa a la estación base de si el paquete ha sido decodificado o no correctamente. Por su parte, el CQI (*Channel Quality Information*) es un índice que informa al *scheduler* de la estación base sobre la tasa de datos en la cual el terminal espera recibir los datos en un instante determinado en función de distintos parámetros de calidad del enlace radio. El canal HS-DPCCH utiliza un factor de ensanchamiento fijo de 256 y tiene una estructura tipo 2ms/3slots. El primer *slot* (ranura) se emplea para la información de HARQ mientras que los demás se emplean para el índice CQI. La frecuencia de transmisión del CQI es controlada por el parámetro de sistema *k*. El índice CQI está codificado en una numeración que va del 0 al 30, tal y como puede apreciarse en la Tabla A-I-1. El valor de CQI no se corresponde directamente con el E_c/N_0 (energía recibida por chip de la portadora piloto dividida por la densidad de potencia del ruido) o con la SIR (*Signal to Interference Ratio*) que experimenta el terminal. En su lugar, el valor de CQI se establece en función del entorno multitrayecto, del tipo de terminal, la relación entre la interferencia de la estación base comparada con otras estaciones y la disponibilidad de potencia del nodo B esperable. El *scheduler* tomará en cuenta el valor del CQI para seleccionar un determinado tipo de modulación y número de canales para la siguiente transmisión, tal y como refleja la Tabla A-I-1. A mayor CQI, mayor es la calidad del enlace y por tanto, más eficiente es la transmisión ya que determina la máxima combinación de tamaño del bloque de transporte, del tipo de modulación y del número de códigos de canalización que se puede emplear. El objetivo es que la transmisión de cada ranura se haga con la configuración óptima en función de las condiciones del canal radio, de la red y de la clase de terminal. En este contexto, se ha fijado el criterio de establecer un CQI mínimo para que un nodo pueda actúar como nodo híbrido. Para implementar este mecanismo, los nodos en el simulador deben ser capaces de obtener valores orientativos del CQI que experimentan.

Valor de CQI	Tamaño de Bloque de Transporte [bits]	Número de HS-PDSCH	Modulación
0	-	-	-
1	137	1	QPSK
2	173	1	QPSK
3	233	1	QPSK
4	317	1	QPSK
5	377	1	QPSK
6	461	1	QPSK
7	650	2	QPSK
8	792	2	QPSK
9	931	2	QPSK
10	1262	3	QPSK
11	1483	3	QPSK
12	1742	3	QPSK
13	2279	4	QPSK
14	2583	4	QPSK
15	3319	5	QPSK
16	3565	5	16-QAM
17	4189	5	16-QAM
18	4664	5	16-QAM
19	5287	5	16-QAM
20	5887	5	16-QAM
21	6554	5	16-QAM
22	7168	5	16-QAM
23	9719	7	16-QAM
24	11418	8	16-QAM
25	14411	10	16-QAM
26	17237	12	16-QAM
27	17237	12	16-QAM
28	17237	12	16-QAM
29	17237	12	16-QAM
30	17237	12	16-QAM

Tabla A-I-1 Mapeo entre el valor de CQI y parámetros de transmisión de LA

En un despliegue real, los nodos pueden evaluar su valor de CQI en tiempo real y decidir si actúan o no como nodos pasarela. Sin embargo, en ns-2 no ha aparecido una distribución oficial que incluya los protocolos necesarios para simular una red celular HSDPA en el momento de la realización de esta tesis. Por ello, se necesita tener una medida evaluable dentro de la herramienta de simulación por cada nodo que esté correlacionada con el valor promedio esperado de CQI. El parámetro escogido para este fin ha sido el de la distancia entre el nodo y la estación base de la red celular. Si bien el CQI experimentado por el nodo no está determinado exclusivamente por esta distancia, sí es posible establecer una relación estadística. Con el objetivo de hallar esta correlación, se llevó a cabo una campaña de medidas en un entorno real en la que se recogieron datos de la distancia entre nodo y estación base, *throughput* y valor de CQI de cada transmisión. El dispositivo experimental utilizado es un terminal móvil Nokia 6720c con capacidad de comunicación GSM/EDGE y UMTS/HSDPA, y que incluye la aplicación *Nemo Handy*

[57]. *Nemo Handy* es capaz de capturar y monitorizar un gran número de parámetros y medidas de red en conexiones de voz y datos, transferencias FTP/HTTP, HTML y *streaming* de vídeo. El procesamiento de los datos medidos se realizó usando la herramienta profesional *Nemo Outdoor* [140]. Esta herramienta proporciona un conjunto de parámetros clave de rendimiento o KPIs (*Key Performance Indicators*) tales como el *throughput*, el BLER o el propio CQI. La aplicación *Nemo Handy* también proporciona sicnronización espacial y temporal a través de un dispositivo GPS conectado vía *Bluetooth*. La información espacial proporcionada por el GPS permite la georeferenciación de todos los datos procesados.

Las medidas fueron tomadas en la ciudad de Elche, en un entorno urbano. La Figura A-I-2 representa los resultados de la campaña de medidas. Cada punto en la Figura A-I-2 corresponde a una de las medidas tomadas, de las que se representa la distancia a la estación base en el eje *x* y el CQI en el eje *y*.

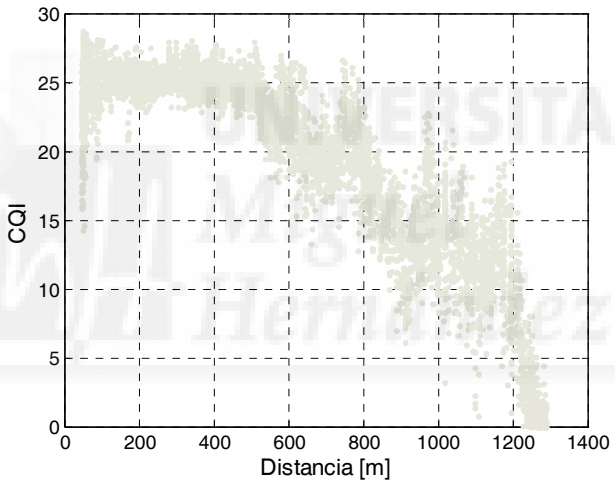


Figura A-I-2. CQI en función de la distancia de campaña de medidas

Teniendo en cuenta estos datos, a continuación se describe el procedimiento para determinar si un nodo, al recibir un paquete de petición de establecimiento de ruta (RREQ), puede o no hacer de nodo híbrido. Se consultó la Tabla A-I-1 para establecer el nivel mínimo de CQI que debe experimentar el nodo para poder actuar como nodo híbrido. La Tabla A-I-1 relaciona el CQI con diversos parámetros de transmisión de la capa física. Uno de estos parámetros es el tipo de modulación. Se utilizan dos tipos de modulación, la 16-QAM y la QPSK. La 16-QAM es superior a la QPSK (permite transmitir más bits por bloque) y por tanto sólo se puede aplicar cuando se alcanza un nivel suficiente CQI, que es de 16. Por ello, este es el valor umbral escogido de CQI para

que un nodo pueda actuar como nodo híbrido[53]. La Figura A-I-3 refleja la probabilidad, para cada intervalo de distancias, de que se cumpla el criterio de un CQI superior a 16. La Figura A-I-3 se ha elaborado tomando 20 intervalos de distancia. Para cada uno de estos intervalos, el punto correspondiente de la Figura A-I-3 representa la probabilidad de que el CQI de las medidas que se tomaron dentro de ese intervalo de distancias sea mayor que 16. Puede observarse que hasta una distancia de 800 metros, la probabilidad de que el CQI sea mayor que 16 es casi del 100% en todo el intervalo, mientras que a partir de dicha distancia hay una caída abrupta. Las parejas de valores formadas por los intervalos de distancia y la probabilidad de obtener un CQI mayor que 16 forma una tabla que permite mapear en el simulador la distancia y la probabilidad de que a esa distancia un nodo pueda actuar como nodo híbrido. Esta tabla ha sido incluida en la plataforma de simulación. De esta manera, cada nodo puede evaluar si actúa o no como nodo híbrido al recibir una petición de establecimiento de ruta, mediante los siguientes pasos:

- Determinación de su distancia a la estación base.
- Determinación del intervalo correspondiente a dicha distancia.
- Selección del valor de probabilidad correspondiente según la tabla representada en la Figura A-I-3.
- Selección de un valor aleatorio *x* y determinación por comparación con el valor de probabilidad anterior si el CQI es superior a 16 y por tanto el nodo puede actuar como híbrido.

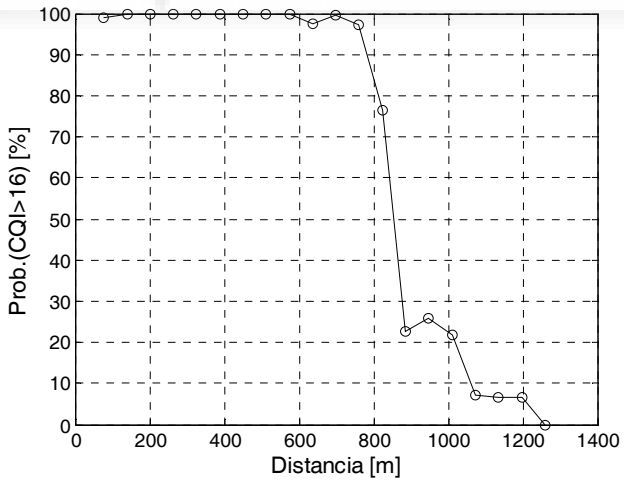


Figura A-I-3. Probabilidad de cumplimiento de requisito de calidad enlace radio.

[53] El criterio escogido por el autor de la tesis, si bien está justificado tal como refleja el texto, no ha sido sacado de ninguna referencia, sino que ha sido seleccionado buscando un procedimiento sencillo e implementable dentro de ns-2.

La funcionalidad para la determinación del nodo pasarela en cada transmisión multi-salto ha sido el único aspecto relacionado con HSDPA que era necesario implementar en ns-2 para poder realizar los experimentos llevados a cabo en el capítulo 8, debido a que la capacidad de descubrimiento y establecimiento de las rutas en la red multi-salto era uno de los principales temas de estudio de la tesis. Por otro lado, no ha sido necesario implementar otras funcionalidades de HSDPA como la transmisión concreta de los paquetes de datos y señalización, ya que no se recoge ningún resultado para el cual deba simularse este aspecto. Simplemente se ha supuesto que los mecanismos de transmisión y de corrección de errores de HSDPA son suficientes para corregir en un tiempo determinado los posibles errores en la comunicación, y por tanto se ha obviado su implementación.

UNIVERSITAS
Miguel
Hernández

A-II

Estimación del parámetro de probabilidad de error p_e

El parámetro p_e representa la probabilidad de error de la técnica de observación *watchdog*, es decir, la probabilidad de que un comportamiento cooperativo (retransmisión correcta del paquete) sea interpretado por el nodo observador como un comportamiento egoísta (no retransmisión del paquete). La razón de este error está en la naturaleza del canal radio, que hace que las comunicaciones inalámbricas estén sujetas a errores de transmisión y colisiones de paquetes. En el capítulo 7 se demostró la necesidad de que los métodos de detección (tanto los Bayesianos como los exponenciales) dispongan de una estimación razonable de la probabilidad de error p_e de la técnica *watchdog*. En los métodos Bayesianos, la estimación de p_e es fundamental para seleccionar el valor adecuado de los parámetros de configuración τ y l, de acuerdo con las Tablas 7-2 y 7-3 del capítulo 7. En los métodos exponenciales, el parámetro p_e aparece explícitamente en la métrica de verosimilitud empleada cuyo valor se compara con el umbral de acusación tras cada observación de descarte. Por tanto, en el capítulo 8, donde se consideran ambos métodos de detección en las simulaciones, se hace necesario implementar un mecanismo para estimar la p_e. El objetivo de este anexo es valorar las distintas alternativas y exponer la que fue adoptada en el presente estudio para los resultados del capítulo 8.

Dado que el valor de p_e puede variar de una transmisión a otra, sería deseable implementar una solución adaptativa. En este contexto, se pueden plantear distintas alternativas. La más inmediata consiste en suponer un valor constante de p_e, basándose en estudios o simulaciones preliminares. Esta solución no sería adaptativa pero es la más sencilla de implementar, siempre y cuando se utilice un valor promedio de p_e adecuado a las condiciones específicas del escenario, y asumiendo las consecuencias del error que se cometerá en la estimación. Dando un paso más allá, podría implementarse alguna técnica como las presentadas en [51] o [52] para estimar un valor de p_e que se ajustase a la mayoría de las transmisiones. Por último, podría aprovecharse de nuevo las potencialidades ofrecidas por la red celular para estimar, mediante la técnica *SC*, el valor de p_e de algunas transmisiones, tal y como se explicaba en el apartado 8.2. En todos los casos, se incurre siempre en un cierto error en la estimación. Ya se estudió en el apartado 7.3.4 cómo afectaba a la capacidad de detección de las técnicas bayesianas y exponenciales el error en la estimación. El efecto más llamativo sobre el proceso de detección de una desviación en la estimación se apreciaba al infravalorar la probabilidad de error, es decir, usar una estimación de p_e menor de la real. Esto podía provocar un incremento considerable de las acusaciones incorrectas (Figura 7-15). En el presente trabajo se ha optado en una primera aproximación por la solución más sencilla, suponer un valor constante. También se ha implementado una versión preliminar de un algoritmo heurístico, presentado en la sección 8.2, en el que el valor estimado de la p_e es ajustado dinámicamente tras cada proceso de la técnica SC.

Para llevar a cabo la primera de las estrategias mencionadas, utilizar un valor constante de p_e para cada método de detección, es necesario conocer cuál es el más adecuado a las condiciones específicas de la red. En el caso del capítulo 8 vienen determinadas por la configuración de los parámetros de simulación reflejados en la Tabla 8-1. El criterio que ha sido utilizado para escoger el valor adecuado de p_e es seleccionar aquél con el que, aplicando las técnicas BC+SC propuestas en el capítulo 8, se obtenga un mejor rendimiento en términos de conectividad para los nodos cooperativos y aislamiento para los nodos que no son cooperativos. Para ello se evaluó el parámetro de PDR, dado que proporciona una visión global del funcionamiento de la red en cuanto a paquetes entregados procedentes de nodos egoístas y de nodos cooperativos, como ya se ha visto en el capítulo 8. Si bien en el capítulo 7 se empleaba otro criterio, el de precisión y rapidez de detección, hay que recordar que en dicho capítulo únicamente se evaluaba el rendimiento de los métodos de detección Bayesianos y exponenciales, y no el funcionamiento íntegro de una técnica de reputación en una red MCN, como en el capítulo 8, y por tanto no podía tenerse en cuenta el grado de aislamiento de los nodos egoístas conseguido. Además, el criterio basado en el PDR recoge indirectamente también los parámetros de precisión y rapidez de las técnicas de detección. Más

concretamente, el criterio de selección de p_e constante para ser utilizado en las simulaciones es escoger el que maximiza el valor del PDR de los nodos cooperativos (p_s=0), con la restricción de que el PDR de los nodos con un p_s>0.5 deberá ser menor que un 10%[54].

En las Figuras A-II-1 a A-II-8 se muestra el PDR para algunos de los métodos de detección bayesianos y exponenciales (BIW, BDF, EIW y EFW) presentados en el capítulo 7 frente a la probabilidad de egoísmo del nodo p_s. Cada una de las curvas de las figuras representa un valor diferente de la estimación de p_e. En las Figuras A-II-1 a A-II-4 se ha considerado el escenario con un nivel de conectividad reducido de los dos propuestos en el apartado 8.3.3, mientras que el segundo escenario con mayor conectividad se considera en las Figuras A-II-5 a A-II-8. En todas las figuras se han aplicado las mejoras BC y SC a la vez para que pueda apreciarse sobre el PDR el efecto de emplear un método de detección u otro. Por último, la etiqueta "p_e var." hace referencia al algoritmo de ajuste dinámico de p_e explicado en el apartado 8.2. El PDR de los nodos cooperativos puede leerse en el punto p_s=0, mientras que el PDR de los nodos egoístas corresponde a los puntos en que p_s>0.

Se pueden extraer distintas conclusiones del análisis de las Figuras A-II-1 a A-II-8. En las cuatro figuras del escenario I (A-II-1 a A-II-4) se observa que el PDR de los nodos cooperativos aumenta al elevar la p_e hasta un valor, a partir del cual ya no tiene sentido elevar más la p_e, puesto que el PDR de los nodos cooperativos no aumenta más, es el nivel máximo de conectividad alcanzable para los nodos (compárese con las técnicas de referencia en Figuras 8-9 y 8-10). Es más, resulta contraproducente, puesto que elevar la p_e también aumenta el PDR de los nodos egoístas. Esta tendencia es fácilmente explicable recordando el análisis de la sensibilidad de la detección al error en la estimación de p_e realizado en el capítulo 7. Cuando se estimaba una p_e por debajo del valor real de p_e, la tasa de acusaciones incorrectas aumentaba considerablemente. Por ello, cuando la estimación de p_e es muy baja, esto resulta en que el proceso de detección genera un número elevado de acusaciones incorrectas, lo cual hace que nodos cooperativos sean aislados incorrectamente y su PDR descienda, dado que se emplean las técnicas de BC y SC, que permiten aislar completamente a los nodos que son acusados de un comportamiento egoísta. Este efecto puede apreciarse en todas las técnicas de detección bayesianas y exponenciales, y en ambos escenarios, con mayor y menor conectividad. El

[54] Aislar completamente a los nodos menos egoístas (p_s<0.5) puede ser perjudicial, ya que si la densidad de nodos es reducida, y la disponibilidad de rutas seguras también, los nodos poco egoístas pueden contribuir a la conectividad de la red, dado que descartan pocos paquetes. Por otro lado, exigir que los nodos más egoístas (p_s>0.5) estén completamente aislados, con un PDR=0, es poco realista. El margen del 10% de PDR para los nodos con p_s=0.5 (para los nodos con p_s>0.5 el PDR siempre es menor que para los nodos con p_s=0.5) es razonable, ya que exigir un PDR menor podría aumentar la tasa de *IA* y con ello mermar el PDR de los nodos cooperativos.

esquema con p_e adaptativo obtiene un rendimiento muy irregular en su actual configuración y debe ser estudiado más profundamente para poder perfeccionar su funcionamiento.

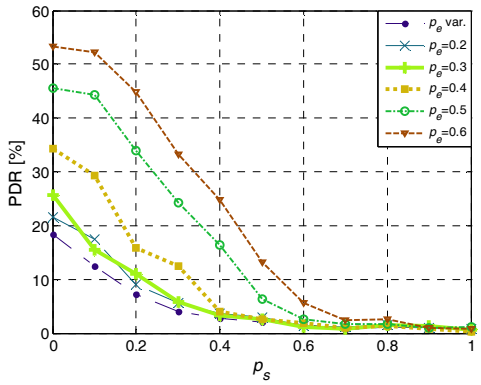


Figura A-II-1. PDR de la técnica BIW con distintas configuraciones de p_e en escenario I.

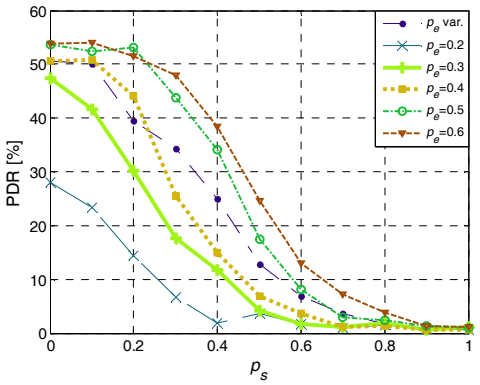


Figura A-II-2. PDR de la técnica BDF con distintas configuraciones de p_e en escenario I.

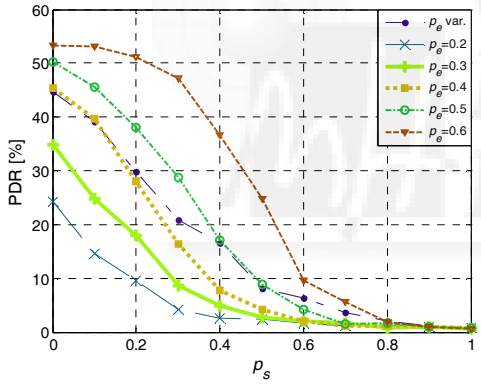


Figura A-II-3. PDR de la técnica EIW con distintas configuraciones de p_e en escenario I.

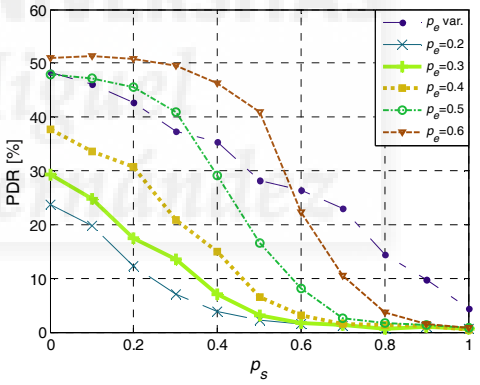


Figura A-II-4. PDR de la técnica EFW con distintas configuraciones de p_e en escenario I.

Por otro lado, no es posible aislar completamente a los nodos con un egoísmo bajo. Estos nodos son más difíciles de detectar, como se vio en el capítulo 7 y en el apartado 8.3.6. Es difícil incluso cuando se selecciona un valor de p_e muy reducido, que como se ha comentado, incrementa el número detecciones. Sin embargo, debe aclararse que no es tan perjudicial que una cierta proporción de nodos con un egoísmo bajo no sean detectados, ya que el número de paquetes que descartan no es muy elevado (Figuras 8-37 y 8-38 en capítulo 8). Además, en caso de que las circunstancias del escenario sólo permitan una conectividad reducida (como en el escenario I), los nodos con un egoísmo

reducido contribuyen a elevar la conectividad de la red (comparar con la Figura 8-9 en el capítulo 8).

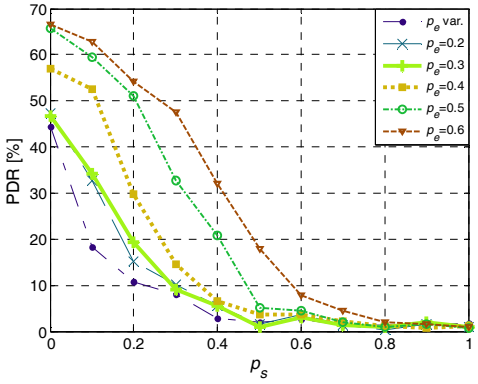


Figura A-II-5. PDR de la técnica BIW con distintas configuraciones de p_e en escenario II.

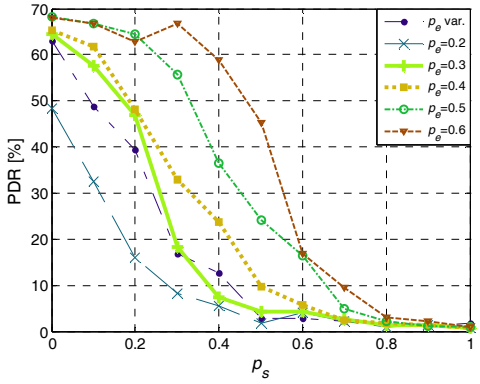


Figura A-II-6. PDR de la técnica BDF con distintas configuraciones de p_e en escenario II.

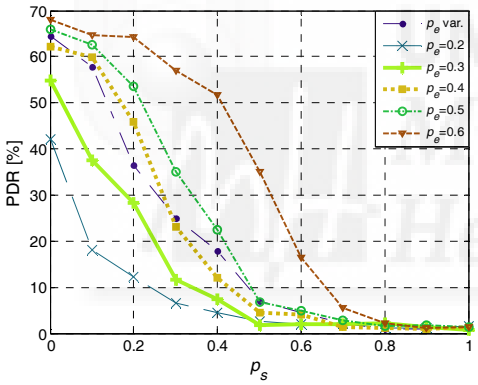


Figura A-II-7. PDR de la técnica EIW con distintas configuraciones de p_e en escenario II.

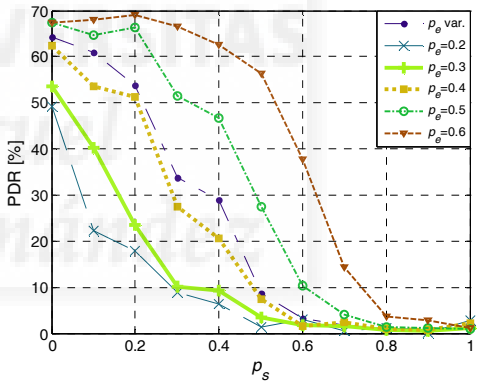


Figura A-II-8. PDR de la técnica EFW con distintas configuraciones de p_e en escenario II.

Para la Figuras A-II-5 a A-II-8, correspondientes al escenario de mayor conectividad, pueden apreciarse las mismas tendencias mencionadas para las figuras anteriores. La principal diferencia, como era esperable, es que los nodos cooperativos obtienen un PDR mayor, debido a una mayor potencia de transmisión y a una menor proporción de nodos egoístas. Además, en ambos escenarios coinciden los valores de p_e que cumplen el criterio de selección establecido: escoger el valor de p_e que permita obtener el mayor PDR para los nodos cooperativos siempre que el PDR de los nodos con un p_s>0.5 sea inferior a un 10%. Este criterio de selección da como resultado el valor de p_e=0.5 para las técnicas BIW y BFW y de p_e=0.4 para las técnicas BDF y EFW. La Tabla 8-5 muestra los valores de (p_e,τ,l) seleccionados finalmente para cada técnica.

	p_e	τ	l
BIW	0.5	0.75	12
BDF	0.4	0.7	12
EIW	0.5	0.35	6
EFW	0.4	0.1	3

Tabla A-II-1. Valores seleccionados de p_e, τ y l empleados en las simulaciones del capítulo 8

Es necesario hacer un inciso para justificar el hecho de que los valores óptimos de p_e seleccionados para cada técnica difieran entre sí. Si se selecciona un valor de p_e=0.5 en las técnicas BDF y EFW, el PDR de los nodos egoístas con p_s=0.5 es superior al límite de 10% que se ha fijado, y por ello se ha seleccionado un p_e inferior en estos casos. La Figura A-II-9 muestra la CDF de los valores de p_e experimentados durante las simulaciones. Los valores de p_e se han calculado empleando la expresión 8-2. Dicha expresión permite calcular la p_e experimentada durante un proceso de detección, a partir de los valores característicos extraídos del proceso de detección (paquetes recibidos correctamente n_R, paquetes observados como descartados α, número total de paquetes n, etc.). El parámetro p_e calculado de esta manera toma valores aproximadamente uniformes, aunque escalonados, entre 0 y 1, como muestra la Figura A-II-9. Se deduce de ello que al escoger un valor constante de la estimación de la p_e para toda la simulación, se comete siempre un cierto error. En las Figuras 7-15 y 7-16 del capítulo 7 se mostraba la sensibilidad de la precisión de cada método de detección a la desviación de la estimación de la p_e, respecto al valor de la p_e real. La desviación de la estimación se medía con el parámetro de error ε_{pe}:

$$\varepsilon_{pe} = \frac{p_e - \hat{p}_e}{\hat{p}_e} \tag{A-II-1}$$

De aquellas gráficas puede concluirse que sobreestimar el valor de p_e (ε_{pe} negativa), aumentaba ligeramente el error por no detectar a los nodos egoístas (*INA Incorrect No Accusations*, Figura 7-16). Es decir, provoca que el sistema sea menos capaz de aislar a los nodos egoístas. Por el contrario, subestimar el valor de p_e (ε_{pe} positiva), consigue el efecto contrario, aumenta el error por acusar a nodos cooperativos (*IA Incorrect Accusations*, Figura 7-15), y este incremento es más acusado que el que se produce en la *INA* al sobreestimar el valor de p_e. Debido al error cometido al suponer una p_e constante, y a la sensibilidad de los métodos de detección a este error, resulta dificultoso distinguir a los nodos con un egoísmo reducido ($0<p_s<0.5$) de los nodos cooperativos, y también conseguir aislarlos adecuadamente sin perjudicar a los nodos cooperativos.

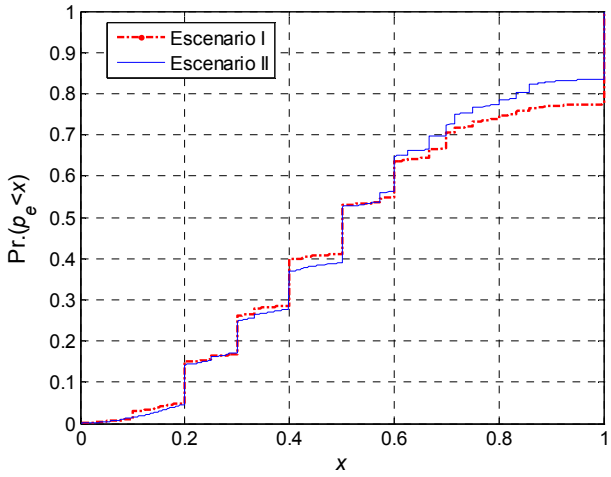


Figura A-II-9. CDF de la estimación del parámetro p_e experimentado.

UNIVERSITAS
Miguel
Hernández

Bibliografía

[1] M. Conti y S. Giordano, "Multihop Ad Hoc Networking: The Theory", *IEEE Communications Magazine*, vol. 45, núm. 4, pgs. 78-86, Abril 2007.

[2] 3GPP TS 45.001 ver. 11.0.0 Rel-11, "Physical layer on the radio path; General description", 12/09/2012.

[3] IEEE 802.11-1997 "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications", 26/06/1997.

[4] A. Jamalipour y S. Tekinay, "Fourth Generation Wireless Networks and Interconnecting Standards," *IEEE Personal Communications,* vol. 8, núm. 5, Octubre 2001.

[5] IEEE 802.11s "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Amendment Mesh Networking", 2008.

[6] 3GPP TS 21.101 ver. 11.0.0 Rel-11, "Universal Mobile Telecommunications System (UMTS); Technical Specifications and Technical Reports for a UTRAN-based 3GPP system", 06/03/2013.

[7] RFC 3561: "Ad hoc On-Demand Distance Vector (AODV) Routing" http://www.ietf.org/rfc/rfc3561.txt

[8] IEEE P802.11 Wireless LANs. HWMP Specification, 13/11/2006.

[9] W. Stallings, "Local & Metropolitan Area Networks", Prentice Hall, New York, 1996.

[10] G. Su, Z. Han, M. Wu y K.J.R. Liu, "Multiuser cross-layer resource allocation for video transmission over wireless Networks", *IEEE Network*, vol. 20, núm. 2, pgs. 21-27, Marzo-Abril 2006.

[11] P. Giacomazzi, L. Musumeci, G. Caizzone, G. Verticale, G. Liggieri, A. Proietti y S. Sabatini, "Quality of Service for Packet Telephony over Mobile Ad Hoc Networks", *IEEE Network*, vol. 20, núm. 1, pgs. 12-20, Enero-Febrero 2006.

[12] C-C Chou, D.S.L. Wei, C.-C.J. Kuo y K. Naik, "An efficient anonymous communication protocol for peer-to-peer applications over mobile ad-hoc Networks", *IEEE Journal on Selected Areas in Communications*, vol. 25, núm. 1, pgs. 192-203, Enero 2007.

[13] L. Li y L. Lamont, "Support of multimedia SIP applications in mobile ad hoc networks: service discovery and networking architecture", *Libro de Actas del IEEE Global Telecommunications Conference GLOBECOM '05*, Otawa (Canadá), vol. 6, pgs. 3682-3686, Diciembre 2005.

[14] M. Conti y S. Giordano, "Multihop Ad-hoc Networking: The Reality", *IEEE Communications Magazine 2007*, vol. 45, núm. 4, pgs. 88-95, Abril 2007.

[15] R. Bruno, M. Conti y E. Gregori "Mesh Networks: Commodity Multihop Ad Hoc Networks", *IEEE Communications Magazine*, Marzo 2005, pgs.123–131.

[16] Miguel Sepulcre "Adaptive Communication Protocols for Cooperative Vehicular Systems". *Tesis Doctoral*, Departamento de Ingeniería de Comunicaciones, Universidad Miguel Hernández, Mayo 2010.

[17] IEEE 802.11b, "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Higher Speed Physical Layer Extension in the 2.4 GHz band" 16/09/1999.

[18] IEEE 802.11a "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: High-speed Physical Layer in the 5 GHZ Band", 16/09/1999.

[19] F.A. Tobagi y L. Kleinrock, "Packet Switching in Radio Channels: Part II", *IEEE Transactions on Communications*, núm. 23, pgs. 1417-1433, 1975.

[20] Wiki ns-2: http://nsnam.isi.edu/nsnam/index.php/Main_Page.

[21] http://nsnam.isi.edu/nsnam/index.php/Contributed_Code

[22] S. Bajaj, L. Breslau, D. Estrin, K. Fall, S. Floyd, P. Haldar, M. Handley, A. Helmy, J. Heidemann, P. Huang, S. Kumar, S. McCanne, R. Rejaie, P. Sharma, K. Varadhan, Y. Xu, H. Yu y D. Zappala., "Improving simulation for network research". *Technical Report 99-702b*, USC, Marzo 1999. (revisado Septiembre 1999).

[23] J.K. Ousterhout, "Integration: A New Style of Programming", *IEEE Computer*, vol. 32, núm. 5, pg. 53, Mayo 1999.

[24] CMU"s Monarch group: http://www.monarch.cs.rice.edu/

[25] C. Perkins e I. Chakeres, "Dynamic MANET On-demand (AODVv2) Routing" http://tools.ietf.org/html/draft-ietf-manet-dymo-26

[26] WINNER, "D1.1.1. WINNER II interim channel models", Public Deliverable: http://www.ist-winner.org/index.html

[27] M. Sepulcre, "Sistemas Cooperativos de Comunicaciones Móviles tipo Ad-Hoc entre Vehículos para Mejora de la Seguridad Vial", Trabajo de Investigación, *Programa de Doctorado Tecnología de las Comunicaciones de la Universidad Miguel Hernández*, Elche, 2007.

[28] Choudhury S. y Gibson J.D, "Joint PHY/MAC Based Link Adaptation for Wireless LANs with Multipath Fading", *Libro de Actas del IEEE Wireless Communications and Networking Conference*, vol. 2, pgs. 757-762, 2006.

[29] UMTS 30.03 v3.2.0 TR 101 112 "Selection procedures for the choice of radio transmission technologies of the UMTS", ETSI, Abril, 1998.

[30] Matlab: http://www.mathworks.com/

[31] K. Maeda, A.Uchiyama, T. Umedu, H. Yamaguchi, K. Yasumoto y T. Higashino, "Urban pedestrian mobility for mobile wireless network simulation", *Ad Hoc Networks*, vol. 7, núm. 1, pgs. 153-170, 2009.

[32] Q. He, D. Wu, y P. Khosla, "A Secure Incentive Architecture for Ad Hoc Networks. *Wireless Communications and Mobile Computing*, vol. 6, núm. 3, pgs. 333-346, 2006.

[33] T.V.P. Sundararajan y A. Shanmugam, "Modeling the Behavior of Selfish Forwarding Nodes to Stimulate Cooperation in MANET", *International Journal of Network Security & Its Applications (IJNSA)*, vol. 2 núm. 2, pgs. 147-160, 2010.

[34] L. Xu, Z. Lin y A. Ye, "Analysis and Countermeasure of Selfish Node Problem in Mobile Ad Hoc Network", *Libro de Actas de la 10th International Conference on Computer Supported Cooperative Work in Design*, Nanjing (China), pgs. 1-4, 3-5 Mayo 2006.

[35] C.K Toh, K. Dongkyun, O. Sutaek y Y. Hongseok, "The controversy of Selfish nodes in ad hoc networks", *The 12th International Conference on Advanced Communication Technology (ICACT) 2010*, Gangwon-Do (Korea) vol.2, pgs.1087-1092, 7-10 Feb. 2010.

[36] M. Hollick, J. Schmitt, C. Seipl y R. Steinmetz, "On the Effect of Node Misbehavior in Ad Hoc Networks", *Libro de Actas del IEEE International Conference on Communications ICC 2004*, París (Francia), vol. 6, pgs. 3759-3763, 20-24 Junio 2004.

[37] Y. Younghwan y D.P. Agrawal, "Why does it pay to be selfish in a MANET?", *IEEE Wireless Communications*, vol.13, núm. 6, pgs. 87-97, Diciembre 2006.

[38] D. Djenouri y N. Badache, "On eliminating packet droppers in MANET: A modular solution", *Ad Hoc Networks*, vol. 7, núm. 6, pgs. 1243-1258, Agosto 2009.

[39] A. Nadeem y M. Howarth. "Protection of MANETs from a range of attacks using an intrusion detection and prevention system", *Telecommunication Systems*, 27 Julio 2011.

[40] S. Marti, T.J. Giuli, K. Lai y M. Baker, "Mitigating Routing Misbehavior in Mobile Ad-hoc Networks", *Libro de Actas del ACM International Conference on Mobile Computing and Networking MobiCOM*, pgs. 255–265, 2000.

[41] K. Liu, J. Deng, P.K. Varshney y K. Balakrishnan, "An Acknowledgment-based Approach for the Detection of Routing Misbehavior in MANETs", *IEEE Transactions on Mobile Computing*, núm. 6, pgs. 536-550, 2007.

[42] S. Dehnie y S. Tomasin, "Detection of Selfish Nodes in Networks Using CoopMAC Protocol with ARQ", *IEEE Transactions on Wireless Communications*, vol. 9, núm. 7, pgs. 2328-2337, 2010.

[43] P. Michiardi y R. Molva, "Analysis of Coalition Formation and Cooperation Strategies in Mobile Ad Hoc Networks", *Ad Hoc Networks*, vol. 3 núm. 2, pgs. 193-219, 2005.

[44] V. Balakrishnan, V. Varadharajan y U. Tupakula, "Trust Management in Mobile Ad hoc Networks", S. Misra (Ed.), *Guide to Wireless Ad hoc Networks*, *Computer Communications and Networks*, Springer Londres, pgs. 473-502, 2010.

[45] S. Buchegger, C. Tissieres y J.Y. Le Boudee, "A Test-bed for Misbehavior Detection in Mobile Ad-hoc Networks", *Libro de Actas del IEEE Workshop on Mobile Computing Systems and Applications WMCSA*, pgs. 102-111, 2004.

[46] A. Rodriguez-Mayol y J. Gozalvez, "On the Implementation Feasibility of Reputation Techniques for Cooperative Mobile Ad-hoc Networks", *Libro de Actas del European Wireless Conference*, Estambul (Turquía,) pgs. 616–623, 2010.

[47] V. Balakrishnan, V. Varadharajan, U. Tupakula y P. Lucs, "TEAM: Trust Enhanced Security Architecture for Mobile Ad-hoc Networks", *Libro de Actas del 15th ICON IEEE International Conference on Networks 2007*, Adelaida (Australia), pgs. 182-187, 19-21 Noviembre 2007.

[48] T. Zahariadis, H. C. Leligou, P. Trakadas y S. Voliotis, "Trust Management in Wireless Sensor Networks", *European Transactions on Telecommunications*, vol. 21, núm. 4, pgs. 386-395, Junio 2010.

[49] L. Yang, J.M. Kizza, Alma-Cemerlic y F. Liu, "Fine-Grained Reputation-based Routing in Wireless Ad Hoc Networks", *Libro de Actas del IEEE Intelligence and Security Informatics 2007*, New Brunswick (New Jersey), pgs. 75-78, 23-24 Mayo 2007.

[50] S. Buchegger y J.-Y Le Boudec, "A Robust Reputation System for P2P and Mobile Ad-hoc Networks", *Libro de Actas del 2nd Workshop on the Economics of Peer-to-Peer Systems*, Harvard University, 4-5 Junio 2004.

[51] H. Jiang, Y. Yang, J. Xu y L. Wang, "Estimation of Packet Error Rate at Wireless Link of Vanet", *Advances in Wireless Sensors and Sensor Networks, Lecture Notes in Electrical Engineering*; vol. 64, pgs. 329-359, 2010.

[52] B. Han y S. Lee, "Efficient Packet Error Rate Estimation in Wireless Networks", *Libro de Actas del 3rd International ICST Conference on Testbeds and Research Infrastructures for the Development of Networks and Communities 2007*, Orlando (Florida), pgs. 1-9, 21-23 Mayo 2007.

[53] W. Hao, Z. Zhibin y C. Xia, "One Scheme for Cooperation Enhancement in Ad-Hoc Networks", *Libro de Actas de IEEE 64th Vehicular Technology Conference VTC–2006 Fall*, Montreal (Canadá), 25-28 Septiembre 2006.

[54] H. Sun y J. Song, "A Novel Reputation System Facilitating Cooperation in Pervasive Wireless Environment", *Libro de Actas de Canadian Conference on Electrical and Computer Engineering*, Ontario (Canadá), vol. 2, pgs. 951–954, 2-5 Mayo 2004.

[55] G. Bella, G. Constantino y S. Riccobene, "Managing Reputation over MANETs", *Libro de Actas de Fourth International Conference on Information Assurance and Security ISIAS'08*, pgs. 255–260, Septiembre 2008.

[56] H. Holma y A. Toskala, "HSDPA / HSUPA for UMTS", *Wiley*, pg. 43, Junio 2007. ISBN 13 978-0-470-01884-2.

[57] http://www.anite.com/businesses/network-testing/products/nemo-handy

[58] S. Yokoyama, Y. Nakane, O. Takahashi y E. Miyamoto, "Evaluation of the Impact of Selfish Nodes in Ad Hoc Networks and Detection and Countermeasure Methods", *Libro de Actas del 7th International Conference on Mobile Data Management MDM 2006*, Nara (Japón), 10-12 Mayo 2006.

[59] H. Kothari, M. Chaturvedi, "Effect of Selfish Behavior on Power Consumption in Mobile Ad Hoc Network", *Libro de Actas del 32nd Meeting Asia-Pacific Advanced Network 2011*, Nueva Delhi, India, 22-26 Agosto 2011.

[60] Y. Sharma y S. Kumar, "Effect of Power Avaricious Attack on MANET Routing Protocols", *Libro de Actas del 3rd International Conference on Electronics Computer Technology ICECT 2011*, Kanyakumari (India), vol. 4, pgs. 120-123, 8-10 Abril 2011.

[61] L. Santhanam, B. Xie y D.P. Agrawal, "Selfishness in Mesh Networks: Wired Multihop Manets", *IEEE Wireless Comunications*, vol. 15, núm. 4, pgs. 16-23, Agosto 2008.

[62] J.B. Evans, W. Wang y B.J. Ewy, "Wireless Networking Security: Open Issues in Trust, Management, Interoperation and Measurement", *International Journal of Security and Networks*, vol. 1, núm. 1-2, pgs. 84-94, Septiembre 2006.

[63] M.D. Serrat, "Watchdogs colaborativos para la deteccion de nodos maliciosos", Máster de Tesis, UPV, 15 Mayo 2012,

[64] L. Buttyán, J.-P. Hubaux, "Enforcing Service Availability in Mobile Ad-Hoc Networks", *Libro de Actas del 6th Annual International Conference on Mobile Computing and Networking ACM MobiCom 2000*, Boston (Massachusetts), pgs. 87-96, 6-8 Agosto 2000.

[65] L. Buttyán y J.-P. Hubaux, "Stimulating Cooperation in Self-Organizing Mobile Ad Hoc Networks," *Mobile Networks and Applications*, vol. 8, núm. 5, pgs. 579-592, Octubre 2003.

[66] L. Anderegg y S. Eidenbenz, "Ad Hoc-VCG: A Truthful and Cost-Efficient Routing Protocol for Mobile Ad hoc Networks with Selfish Agents", *Libro de Actas del 9th Annual International Conference on Mobile Computing and Networking ACM MobiCom 2003*, Nueva York (Nueva Jersey), pgs. 245-259, 14-19 Septiembre 2003.

[67] S. Zhong, J. Chen y Y. R. Yang, "Sprite: A Simple, Cheat-Proof, Credit-Based System for Mobile Ad-Hoc Networks", *Libro de Actas de la 22nd Annual Joint Conference of the IEEE Computer and Communications Societies IEEE INFOCOM 2003*, San Francisco (California), pgs. 1987-1997, 30 Marzo-3 Abril 2003.

[68] N. B. Salem, L. Buttyán, J.P. Hubaux y Markus Jakobsson, "A Charging and Rewarding Scheme for Packet Forwarding in Multihop Cellular Networks", *Libro de Actas del 4th ACM international symposium on Mobile ad hoc networking and computing 2003*, Nueva York (Nueva Jersey), pgs. 13-24, 14-19 Septiembre 2003.

[69] B. Raghavan y A. C. Snoeren, "Priority Forwarding in Ad Hoc Networks with Self-Interested Parties", *Libro de Actas Workshop of Economics of Peer-to-Peer Systems 2003*, Berkeley, CA, 5-6 Junio 2003.

[70] J. Crowcrof, R. Gibbens, F. Kelly y S. Östring, "Modelling Incentives for Collaboration in Mobile Ad Hoc Networks", *Journal on Selected Papers from the First Workshop on Modeling and Optimization in Mobile, Ad hoc and Wireless Networks WiOpt'2003*, vol. 57, núm. 4, pgs. 427-439, Agosto 2004.

[71] Y. Younghwan, A. Sanghyun y D.P.Agrawal, "A credit-payment scheme for packet forwarding fairness in mobile ad hoc networks", *Libro de Actas IEEE International Conference on Communications ICC 2005*, Seoul (Korea), vol.5, pgs. 3005-3009, 16-20 Mayo 2005.

[72] M. Jakobsson, J.P. Hubaux y L. Buttyán, "A Micro-Payment Scheme Encouraging Collaboration in Multi-Hop Cellular Networks", *Libro de Actas del Financial Criptography Conference 2003*, pgs. 15-33, 2003.

[73] E. Huang, J. Crowcroft y I. Wassell, "Rethinking Incentives for Mobile Ad Hoc Networks", *Libro de Actas del ACM SIGCOMM workshop on Practice and theory of incentives in networked systems PINS'04*, Portland (Oregon), pgs. 191-196, Agosto 30 - 3 Septiembre 2004.

[74] A. Weyland, T. Braun, "CASHnet - Cooperation and Accounting Strategy for Hybrid Networks", *Libro de Actas del 13th IEEE Workshop on Local and Metropolitan Area Networks LANMAN 2004*, pgs. 193-198, 28 Abril 2004.

[75] A. Weyland, T. Staub y T. Braun, "Comparison of Incentive-based Cooperation Strategies for Hybrid Networks", *Wired/Wirless Internet*, Springer Berlin, Hidelberg, 2005.

[76] M.M.E.A. Mahmoud y X. Shen, "FESCIM: Fair Efficient and Secure Cooperation Incentive Mechanism for Multihop Cellular Networks" *IEEE Transactions on Mobile Computing*, vol. 11, núm. 5, pgs. 753-766, Mayo 2012.

[77] L. Buttyán y J. Hubaux "Security and Cooperation in Wireless Networks", Cambridge University Press, 2007.

[78] M.H. Lin y C.-C. Lo,"A Location-based Incentive Pricing Scheme for Tree-based Relaying in Multi-hop Cellular Networks", *Libro de Actas del 9th IFIP/IEEE International*

Symposium on Integrated Network Management IM 2005, Niza (Francia), pgs. 339-352, 15-19 Mayo 2005.

[79] H. Zhu, X. Lin, R. Lu, Y. Fan y X. Shen, "SMART A Secure Multilayer Credit-Based Incentive Scheme for Delay-Tolerant Networks", *IEEE Transactions on Vehicular Technology*, vol. 58, núm. 8, pgs. 4628-4639, Octubre 2009.

[80] M.E. Mahmoud y X. Shen, "Stimulating Cooperation in Multi-hop Wireless Networks Using Cheating Detection System" *Libro de Actas del 29th International Conference on Information Communications IEEE INFOCOM 2010*, San Diego (California), pgs. 1-9.

[81] P. Michiardi y R. Molva, "A Game Theoretical Approach to Evaluate Cooperation Enforcement Mechanisms in Mobile Ad Hoc Networks", *Libro de Actas del Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks WiOpt 2003*, Sophia-Antipolis (Francia), 3-5 Marzo 2003.

[82] P. Michiardi y R. Molva, "Core: a Collaborative Reputation Mechanism to Enforce Node Cooperation in Mobile Ad hoc Networks" *Libro de Actas del Proceedings of the IFIP TC6/TC11 6th Joint Working Conference on Communications and Multimedia Security: Advanced Communications and Multimedia Security 2002*, Portoroz (Eslovenia), pgs. 107-121, 26-27 Septiembre 2002.

[83] M. Felegyhazi, J-P Hubaux y L. Buttyan, "Nash Equilibria of Packet Forwarding Strategies in Wireless Ad Hoc Networks", *IEEE Transactions on Mobile Computing*, vol. 5, núm. 5, pgs. 463-476, Mayo 2006.

[84] R. Mahajan, M. Rodrig, D. Wetherall, y J. Zahorjan, "Sustaining Cooperation in Multi-hop Wireless Networks", *Libro de Actas del 2nd Symposium on Networked Systems Design & Implementation NSDI 2005*, Boston (Massachusetts), vol. 2, pgs. 231-244, 2-4 Mayo 2005.

[85] A. Mok, B. Mistry, E. Chung, y B. Li, "FAIR: Fee arbitrated incentive architecture in wireless ad hoc networks", *Libro de Actas del 10th IEEE Symposium on Real-Time and Embedded Technology and Applications RTAS 2004*, Toronto (Canadá), pgs. 38-47, 25-28 Mayo 2004.

[86] M. Félegyházi, L. Buttyán y J.P. Hubaux, "Equilibrium analysis of packet forwarding strategies in wireless ad hoc networks–the static case", *Libro de Actas del Personal Wireless Communications PWC'03*, Venecia (Italia), pgs. 776-789, January 2003.

[87] A. Urpi, M. Bonuccelli y S. Giordano, "Modelling cooperation in mobile ad hoc networks: a formal description of selfishness", *Libro de Actas del Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks WiOpt'03*, Sophia-Antipolis (Francia), 3-5 Marzo 2003.

[88] V. Srinivasan, P. Nuggehalli, C.F. Chiasserini y, R.R. Rao, "Cooperation in wireless ad hoc networks", *Libro de Actas del 22nd Annual Joint Conference of the IEEE Computer and Communications IEEE Societies INFOCOM 2003*, San Francisco (California), vol. 2, pgs. 808-817, 30 Marzo - 3 Abril 2003.

[89] S. Zhong , L. Li, Y.G. Liu y Y.R. Yang, "On designing incentive-compatible routing and forwarding protocols in wireless ad-hoc networks: an integrated approach using game theoretic and cryptographic techniques", *Wireless Networks*, vol. 13, núm. 6, pgs. 799-816, 2007.

[90] J.J. Jaramillo y R. Srikant, "DARWIN: distributed and adaptive reputation mechanism for wireless ad-hoc networks", *Libro de Actas del 13th Annual ACM International Cconference on Mobile Computing and Networking MobiCom 2007*, Montréal (Cánada), pgs. 87-98, 9-14 Septiembre 2007.

[91] S. Zhong y F. Wu, "On designing collusion-resistant routing schemes for non-cooperative wireless ad hoc networks", *Libro de Actas del 13th Annual ACM International Cconference on Mobile Computing and Networking MobiCom 2007*, Montréal (Cánada), pgs. 278-289, 9-14 Septiembre 2007.

[92] F. Milan, J.J. Jaramillo y R. Srikant, "Performance Analysis of Reputation-based Mechanisms for Multi-hop Wireless Networks", *Libro de Actas del 40th Annual Conference on Information Sciences and Systems CISS 2006*, Princeton (Nueva Jersey), pgs. 12-17, 22-24 Marzo 2006.

[93] S.K. Ng y W.K.G. Seah, "Game-theoretic model for collaborative protocols in selfish, tariff-free, multihop wireless networks", *Libro de Actas del 27th Conference on Computer Communications INFOCOM 2008*, Phoenix (Arizona), pgs. 216-220, 13-18 Abril 2008.

[94] W. Wang, M. Chatterjee y K. Kwiat "Enforcing cooperation in ad hoc networks with unreliable channel", *Libro de Actas del 5th IEEE International Conference on In Mobile Ad Hoc and Sensor Systems MASS 2008*, Atlanta (Georgia), pgs. 456-462, 29 Septiembre - 2 Octubre 2008.

[95] Y. Wu, S. Tang, P. Xu y X.Y. Li, "Dealing with selfishness and moral hazard in noncooperative wireless networks", *IEEE Transactions on Mobile Computing*, vol. 9, núm 3, pgs. 420-434, 2010.

[96] C. Crepeau, C.R. Davis y M. Maheswaran, "A secure MANET routing protocol with resilience against byzantine behaviours of malicious or selfish nodes", *Libro de Actas del 21st International Conference on Advanced Information Networking and Applications Workshops AINAW'07*, Ontario (Canadá), vol. 2, pgs. 19-26, 21-23 Mayo 2007.

[97] C. Song y Q. Zhang, "COFFEE: a context-free protocol for stimulating data forwarding in wireless ad hoc networks", *Libro de Actas del 6th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks SECON'09*, Roma (Italia), pgs. 1-9, 22-26 Junio 2009.

[98] D. Qian, C. Zhou y J. Zhang, "Cooperation enforcement in ad hoc networks with penalty", *Libro de Actas del IEEE International Conference on Mobile Adhoc and Sensor Systems Conference MASS 2005*, Washington, DC, pgs. 179-185, 7-10 Noviembre 2005.

[99] M.M. Islam, R. Pose y C. Kopp "An Intrusion Detection System for Suburban Ad-hoc Networks", *Libro de Actas del IEEE Region 10 International Conference TENCON 2005*, Melbourne (Australia), pgs. 1-6, 21-24 Noviembre 2005.

[100] B. Bhargava, X. Wu, Y. Lu y W. Wang, "Integrating heterogeneous wireless technologies: a cellular aided mobile ad hoc network (CAMA)", *Mobile Networks and Applications*, vol. 9, núm. 4, pgs. 393-408, 2004.

[101] M.T. Refaei, Y. Rong, L.A. DaSilva y H.A. Choi, "Detecting node misbehavior in ad hoc networks", *Libro de Actas del IEEE International Conference on Communications ICC'07*, Glasgow (Escocia), pgs. 3425-3430, 24-28 Junio 2007.

[102] P. Michiardi y R. Molva, "Simulation-based analysis of security exposures in mobile ad hoc networks", *Libro de Actas del European Wireless Conference EW2002*, Florencia (Italia), 25-28 Febrero 2002.

[103] S. Capkun, L. Buttyan y J-P. Hubaux, "Self-organized public-key management for mobile ad hoc networks", *IEEE Transactions on Mobile Computing*, vol.2, núm. 1, pgs. 52-64, Enero-Marzo 2003.

[104] P. Papadimitratos y Z.J. Haas, "Secure message transmission in mobile ad hoc networks", *Ad Hoc Networks*, vol. 1, núm. 1, pgs. 193-209, 2003.

[105] P. Kotzanikolaou, R. Mavropodi y C. Douligeris, "Secure Multipath Routing for Mobile Ad Hoc Networks", *Libro de Actas del 2nd Annual Conference on Wireless On-demand Network Systems and Services WONS 2005*, St. Moritz (Suiza), pgs. 89-96, 19-21 Enero 2005.

[106] P. Papadimitratos y Z.J. Haas, "Secure routing for mobile ad hoc networks", *Libro de Actas del Commnication Networks and Distributed Systems Modeling and Simulation Conference CNDS 2000*, pgs. 193-204, 2000.

[107] K. Wang, M.Wu, P. Xia; S. Xie, W. Lu y S. Shen, "A secure authentication scheme for integration of cellular networks and MANETs", *Libro de Actas del International Conference on Neural Networks and Signal Processing*, Zhenjiang (China), pgs. 315-319, 7-11 Junio 2008.

[108] M. Omar, Y. Challal y A. Bouabdallah, "NetTRUST: mixed networks trust infrastructure based on threshold cryptography", *Libro de Actas del IEEE 3rd International Conference on Security and Privacy in Communications Networks and the Workshops SecureComm 2007*, pgs. 2-10, Septiembre 2007.

[109] S. Buchegger, J. Mundinger y J.-Y. Le Boudec, "Reputation Systems for Self-Organized Networks", *IEEE Technology and Society Magazine*, vol. 27, núm. 1, pgs. 41-47, Primavera 2008.

[110] J-H. Cho, A. Swami y I-R. Chen, "A Survey on Trust Management for Mobile Ad Hoc Networks", *IEEE Communications Surveys & Tutorials*, vol. 13, núm. 4, pgs. 562-583, Cuarto Trimeste 2011.

[111] K. Paul, D. Westhoff, "Context Aware Detection of Selfish Nodes in DSR based Ad-hoc Networks," *Libro de Actas IEEE GLOBECOM 2002*, Taipei (Taiwán), pgs. 178–82, 17-21 Noviembre 2002.

[112] S. Buchegger y J.-Y. L. Boudec, "Performance Analysis of the CONFIDANT Protocol (Cooperation of Nodes: Fairness In Dynamic Ad-hoc NeTworks)", *Libro de Actas del 3rd ACM International Symposium on Mobile Ad Hoc Networking and Computing MobiHoc 2002*, Lausana (Suiza), pgs. 226–236, 2002.

[113] W. Yau y C.J. Mitchell, "Reputation Methods for Routing Security for Mobile Ad Hoc Networks", *Libro de Actas del Joint 1st Workshop on Mobile Future and Symposium on Trends in Communications SympoTIC'*03, pgs. 130 – 137, 28 Octubre 2003.

[114] W.J. Adams, G.C. Hadjichristofi y N.J. Davis IV, "Calculating a Node's Reputation in a Mobile Ad Hoc Network", *Libro de Actas del 24th IEEE International IEEE International Performance, Computing and Communications Conference IPCCC 2005*, pgs. 303-307, 7-9 Abril 2005.

[115] S. Balfe, P.-W. Yau y K.G. Paterson, "A guide to trust in mobile ad hoc networks", *Security Communications Networks*, vol. 3, núm. 6, pgs. 503-516, 2010.

[116] G. Bigwood y T. Henderson, "IRONMAN: Using Social Networks to Add Incentives and Reputation to Opportunistic Networks", *Libro de Actas del IEEE 3rd International Conference on Privacy, Security, Risk and Trust PASSAT 2011 y del IEEE 3rd International Conference on Social Computing SOCIALCOM 2011*, pgs. 65-72, 9-11 Octubre 2011.

[117] S. Buchegger y J.Y. Le Boudec, "A Robust Reputation System for P2P and Mobile Ad hoc Networks", *Libro de Actas del 2nd Workshop on the Economics of Peer-to-Peer P2PEcon 2004*, Harvard University (Massachusetts), 4-5 Junio 2004.

[118] P.B. Velloso, R.P. Laufer, D. de O Cunha, O.C.M.B. Duarte y G. Pujolle, "Trust management in mobile ad hoc networks using a scalable maturity-based model", *IEEE Transactions on Network and Service Management*, vol. 7, núm. 3, pgs. 172-185, Septiembre 2010.

[119] T. Anker, D. Dolev y B. Hod, "Cooperative and reliable packet-forwarding on top of AODV", *Libro de Actas del 4th International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks WiOpt 2006*, Boston (Massachusetts), pgs. 241-250, 3-7 Abril 2006.

[120] H. Miranda, L. Rodrigues, "Friends and Foes: Preventing Selfishness in Open Mobile Ad Hoc Networks," *Libro de Actas del International Conference on Distributed Computing Systems Workshop 2003*, pgs. 440 – 445.

[121] Y. Liu y Y. R. Yang, "Reputation propagation and agreement in mobile ad-hoc networks", *Libro de Actas del IEEE International Conference on Wireless Communications and Networking WCNC 2003*, vol. 3, pgs. 1510-1515, 20 Marzo 2003.

[122] D. Djenouri, O. Mahmoudi, M. Bouamama, D. Llewellyn-Jones y M. Merabti, "On Securing MANET Routing Protocol Against Control Packet Dropping", *Libro de Actas del IEEE International Conference on Pervasive Services*, pgs. 100-108, 15-20 Julio 2007.

[123] L. Guang y C. Assi, "Mitigating Smart Selfish MAC Layer Misbehavior in Ad Hoc Networks", *Libro de Actas del IEEE International Conference on Wireless and Mobile Computing, Networking and Communications WiMob'2006*, pgs. 116-123, 19-21 Junio 2006.

[124] J. Cai, Y. Liu, J. Lian, Z. Li, U. Pooch y L. Ni, "Truthful Topology Control inWireless Ad Hoc Networks with Selfish Nodes", *Libro de Actas del International Conference on Parallel Processing ICPP 2006*, pgs. 203-210, 14-18 Agosto 2006.

[125] D. Djenouri y N. Badache, "New approach for selfish nodes detection in mobile ad hoc networks", *Libro de Actas del Workshop of the 1st International Conference on Security and Privacy for Emerging Areas in Communication Networks*, pgs. 288-294, 5-9 Septiembre 2005.

[126] Q. Zhang y D.P. Agrawal, "Impact of selfish nodes on route discovery in mobile ad hoc networks", *Libro de Actas del IEEE Global Telecommunications Conference GLOBECOM'04*, vol. 5, pgs. 2914-2918, 29 Noviembre - 3 Diciembre 2004.

[127] J. Sen, P.R. Chowdhury y I. Sengupta, "A Distributed Trust Mechanism for Mobile Ad Hoc Networks", *Libro de Actas del International Symposium on Ad Hoc and Ubiquitous Computing ISAUHC'06*, pgs 62-67, 20-23 Diciembre 2006.

[128] K. Balakrishnan, D. Jing y V. K. Varshney, "TWOACK: Preventing Selfishness in Mobile Ad hoc Networks", *Libro de Actas del Wireless Communications and Networking Conference WCNC'05*, vol. 4, pgs. 2137-2142, Marzo 2005.

[129] K.Vijaya, "Secure 2Ack Routing Protocol In Mobile Ad Hoc Networks" *Libro de Actas del IEEE Region 10 International Conference TENCON 2008*, pgs. 1-7, Noviembre 2008.

[130] S. Usha y S. Radha, "Co-operative Approach to Detect Misbehaving Nodes in MANET using Multi-hop Acknowledgement Scheme", *Libro de Actas de la International Conference on Advances in Computing, Control, and Telecommunication Technologies*, pgs. 576-578, Diciembre 2009.

[131] M. Zeshan, S.A. Khan, A.R. Cheema y A. Ahmed, "Adding Security against Packet Dropping Attack in Mobile Ad Hoc Networks", *Libro de Actas del International Seminar on Future Information Technology and Management Engineering*, pgs. 568-572, Noviembre 2008.

[132] A.S.A. Ukey y M. Chawla, "Detection of Packet Dropping Attack Using Improved Acknowledgement Based Scheme in MANET", *IJCSI International Journal of Computer Science Issues*, vol. 7, núm. 4, pgs. 12-17, Julio 2010.

[133] X. Su, G. Pengy y S. Chan, "FORBID: Cope with Byzantine Behaviors in Wireless Multi-Path Routing and Forwarding", *Libro de Actas del IEEE Global Telecommunications Conference GLOBECOM 2011*, pgs.1-6, 5-9 Diciembre 2011.

[134] J. Hortelano, "Design and Implementation of Architectures for the Deployment Secure Community Wireless Networks", *Tesis Doctoral*, Departamento de Informática de Sistemas y Computadores, Universidad Politécnica de Valencia, 2011.

[135] M. Danzeisen, T. Braun, D. Rodellar y S. Winiker, "Heterogeneous communications enabled by cellular operators", *IEEE Vehicular Technology Magazine*, vol. 1, núm. 1, pgs. 23-30, 2006.

[136] H. Luo, R. Ramjee, P. Sinha, L.E. Li y S. Lu, "UCAN: A Unified Cellular and AdHoc Network Architecture", *Libro de Actas del 9th Annual International Conference on Mobile Computing and Networking MobiCom 2003*, pgs. 353-367, Septiembre 2003.

[137] M. Zhao y W. Wang, "A Unified Mobility Model for Analysis and Simulation of Mobile Wireless Networks", *Wireless Networks*, vol. 15, núm. 3, pgs. 365-389, Septiembre 2007.

[138] M.R. Senouci, A. Derhab y N. Badache, "Efficient Monitoring Mechanisms for Cooperative Storage in Mobile Ad-Hoc Networks: Detection Time and Accuracy Tradeoffs", *Libro de Actas del 29th IEEE International Conference on Distributed Computing Systems Workshops ICDCS Workshops'09*, pgs. 130-136, 22-26 Junio 2009.

[139] J. Sen, M. Chandra, S.G. Harihara, H. Reddy y P. Balamuralidhar, "A mechanism for detection of gray hole attack in mobile ad hoc networks", *Libro de Actas del 6th IEEE International Conference Information, Communications & Signal Processing ICICS'07*, pgs. 1-5, 10-13 Diciembre 2007.

[140] http://www.anite.com/businesses/network-testing/products/nemo-outdoor

[141] T.K. Forde, L.E. Doyle y D. O'Mahony, "Ad hoc innovation: distributed decision making in ad hoc networks", *IEEE Communications Magazine*, vol. 44, núm. 4, pgs. 131-137, Abril 2006.

[142] R. Sivakami y G.M.K. Nawaz, "Secured communication for MANETS in military", *Libro de Actas del International Conference on Computer, Communication and Electrical Technology ICCCET 2011*, pgs. 146-151, 18-19 Marzo 2011.

[143] Y. Gadallah y M.A. Serhani, "A WSN-driven service discovery technique for disaster recovery using mobile ad hoc networks", *Libro de Actas del Wireless Days WD 2011*, pgs. 1-5, 10-12 Octubre 2011.

[144] M. Ilyas, "The Handbook Of Ad Hoc Wireless Networks", *The Electrical Engineering Handbook Series*, CRC Press 2010.

[145] S. Agrawal, S. Jain, S. Sharma y R. Gupta, "Mobility based Performance Analysis of AODV and DYMO under Varying Degree of Node Misbehavior", *International Journal of Computer Applications IJCA*, vol. 30, núm. 7, pgs. 36-41, Septiembre 2011.

[146] RFC 5498: "IANA Allocations for Mobile Ad Hoc Network (MANET) Protocols": https://tools.ietf.org/html/rfc5498

[147] RFC 6130: "Mobile Ad Hoc Network (MANET) Neighborhood Discovery Protocol (NHDP)": https://tools.ietf.org/html/rfc6130

[148] W.H. Tranter, K.S. Shanmugan, T.S. Rappaport y K. L. Kosbar, "Principles of Communication Systems Simulation with Wireless Applications", Prentice Hall PTR, 2003.