



UNIVERSIDAD
DE MÁLAGA



E.T.S. DE INGENIERÍA DE
TELECOMUNICACIÓN
UNIVERSIDAD DE MÁLAGA

PROGRAMA DE DOCTORADO EN INGENIERÍA DE TELECOMUNICACIÓN

Tesis Doctoral

CARACTERIZACIÓN Y ANÁLISIS DE LA PROPAGACIÓN DE CIBERATAQUES JAMMING EN REDES DE SENSORES INALÁMBRICOS MEDIANTE MODELOS EPIDEMIOLÓGICOS

Autor

D. Miguel López Delgado

Directores

Dr. Alberto Peinado Domínguez
(ETSIT – UMA)

Dr. Andrés Ortiz García
(ETSIT – UMA)


Málaga, Junio 2022





UNIVERSIDAD
DE MÁLAGA

AUTOR: Miguel López Delgado

 <https://orcid.org/0000-0002-7145-2296>

EDITA: Publicaciones y Divulgación Científica. Universidad de Málaga



Esta obra está bajo una licencia de Creative Commons Reconocimiento-NoComercial-SinObraDerivada 4.0 Internacional:

<http://creativecommons.org/licenses/by-nc-nd/4.0/legalcode>

Cualquier parte de esta obra se puede reproducir sin autorización

pero con el reconocimiento y atribución de los autores.

No se puede hacer uso comercial de la obra y no se puede alterar, transformar o hacer obras derivadas.

Esta Tesis Doctoral está depositada en el Repositorio Institucional de la Universidad de Málaga (RIUMA): riuma.uma.es



**DECLARACIÓN DE AUTORÍA Y ORIGINALIDAD DE LA TESIS
PRESENTADA PARA OBTENER EL TÍTULO DE DOCTOR**

D. Miguel López Delgado,

Estudiante del programa de doctorado de la Escuela Técnica Superior de Ingeniería de Telecomunicación de la Universidad de Málaga, autor de la Tesis, presentada para la obtención del título de Doctor por la Universidad de Málaga, titulada: *CARACTERIZACIÓN Y ANÁLISIS DE LA PROPAGACIÓN DE CIBERATAQUES JAMMING EN REDES DE SENSORES INALÁMBRICOS MEDIANTE MODELOS EPIDEMIOLÓGICOS.*

Realizada bajo la dirección de D. Alberto Peinado Domínguez y de D. Andrés Ortiz García y la tutorización de D. Alberto Peinado Domínguez.

DECLARO QUE:

La tesis presentada es una obra original que no infringe los derechos de propiedad intelectual ni los derechos de propiedad industrial u otros, conforme al ordenamiento jurídico vigente (Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia), modificado por la Ley 2/2019, de 1 de marzo.

Igualmente asumo, ante a la Universidad de Málaga y ante cualquier otra instancia, la responsabilidad que pudiera derivarse en caso de plagio de contenidos en la tesis presentada, conforme al ordenamiento jurídico vigente.

En Málaga, a 20 de Mayo de 2022.

Fdo.: D. Miguel López Delgado

Fdo.: Dr. D. Andrés Ortiz García

Doctorando

Director de Tesis

Fdo.: Dr. D. Alberto Peinado Domínguez

Director y tutor de Tesis



UNIVERSIDAD
DE MÁLAGA

AUTORIZACIÓN DE LOS DIRECTORES PARA LA LECTURA DE LA TESIS

Los doctores Don Alberto Peinado Domínguez y Don Andrés Ortiz García, profesores de la Universidad de Málaga del departamento de Ingeniería de Comunicaciones, de la Escuela Técnica Superior de Ingeniería de Telecomunicación:

Al doctorando, Miguel López Delgado, a la lectura y defensa de su Tesis Doctoral titulada:

CARACTERIZACIÓN Y ANÁLISIS DE LA PROPAGACIÓN DE CIBERATAQUES JAMMING EN REDES DE SENSORES INALÁMBRICOS MEDIANTE MODELOS EPIDEMIOLÓGICOS

de la cual son directores. Además, informan de que los artículos que han servido para justificar este trabajo no han sido usados en otra Tesis.

Y para que así conste, expiden y firman este informe en

Málaga, a 20 de Mayo de 2022.

Fdo.: Dr. D Alberto Peinado Domínguez Fdo.: Dr. D. Andrés Ortiz García

Director y tutor de Tesis

Director de Tesis



UNIVERSIDAD
DE MÁLAGA

Resumen de la Tesis Doctoral

En los últimos años, la adopción de la tecnología de Redes de Sensores Inalámbricos (*Wireless Sensor Networks*, WSN) ha aumentado considerablemente, surgiendo nuevos paradigmas como la Industria 4.0 o el Internet de las Cosas (*Internet of Things*, IoT) entre otros. Sin embargo, debido factores como la naturaleza inalámbrica del canal, la reducida capacidad de procesamiento de los nodos, la dificultad de adoptar en todas las aplicaciones mecanismos de seguridad adecuados, o su despliegue en entornos desatendidos, entre otros, expone a estas redes a diversas amenazas desde el punto de vista de la Ciberseguridad, favoreciendo nuevas formas de ciberataques.

Por lo tanto, las redes de sensores inalámbricos han de afrontar retos más complejos desde el punto de vista de la Ciberseguridad, debiendo ser abordados introduciendo nuevas metodologías y modelos. En este sentido, la adopción de enfoques *bioinspirados*, los cuales se centran en comprender los fundamentos de ciertos sistemas biológicos, captando su comportamiento dinámico para ser posteriormente aplicado a sistemas no biológicos, ofrece un campo de estudio realmente interesante y, por su naturaleza, aplicable a las redes de sensores inalámbricos.

El paralelismo entre el comportamiento de ciertas infecciones biológicas y algunos tipos de ciberataques en redes de comunicaciones, ha atraído a los investigadores en Ciberseguridad en los últimos años, llevando a éstos a aplicar modelos epidemiológicos para estudiar ciertos tipos de ataques contra redes de comunicaciones cableadas e inalámbricas. Desde entonces, se han desarrollado modelos epidemiológicos que han tratado de ajustarse a las características particulares de cada ataque, si bien la mayoría de ellos se centran en el análisis de la propagación de *malware*, lo que implica la necesidad de implementar código de programación o algoritmos para desplegar el ataque, algo que puede no ser posible debido a las limitaciones de los nodos inalámbricos. Sin embargo, existen otro tipo de ciberataques no basados en *malware* ni en programación compleja, que pueden ser ejecutados contra este tipo de redes independientemente de la complejidad de los nodos.

Esta Tesis Doctoral, iniciada en 2016, se basa en la hipótesis de que la propagación de un determinado tipo de ciberataque contra una red de sensores inalámbricos, ha de seguir una dinámica de propagación similar al de la propagación dentro de una población

de humanos, de una enfermedad producida por un patógeno infeccioso o virus transmitido por el aire, tal como la gripe, el SARS o la COVID-19.

El ciberataque a estudio, denominado ataque de interferencia o también conocido como ataque *jamming*, es independiente de la complejidad y potencia de procesamiento de los dispositivos afectados. Este enfoque de análisis de los ciberataques se enmarca en el concepto de sistemas *bioinspirados*, mencionados anteriormente, y para ello se propone la utilización de los modelos matemáticos empleados en la Teoría Epidemiológica moderna, los cuales se emplean para estudiar y analizar la propagación de enfermedades infecciosas, buscando parones de comportamiento y midiendo su incidencia en una población objetivo.

El objetivo principal de esta Tesis Doctoral es diseñar, desarrollar y proponer nuevas metodologías y modelos que permitan mejorar la Ciberseguridad de las redes de sensores inalámbricos y reducir así el riesgo asociado a un ciberataque en este tipo de redes, bien reduciendo el factor de probabilidad de riesgo, reduciendo el factor de impacto, o ambos a la vez.

A lo largo de los diferentes Capítulos de esta Tesis se aborda la aplicación de diferentes modelos epidemiológicos para la caracterización y análisis de ataques tipo *jamming* aleatorio y reactivo contra redes de sensores inalámbricos, siguiendo los pasos propios de la investigación de brotes epidémicos. Este enfoque epidemiológico se ha validado mediante una serie de experimentos sobre diferentes escenarios de ataque, siendo comparados los resultados experimentales con un conjunto de datos de referencia.

En general, los resultados obtenidos indican que los diferentes modelos epidemiológicos propuestos en esta Tesis han permitido determinar diferentes perfiles de crecimiento de las curvas características de los ataques *jamming*, incluso en un contexto de datos empíricos limitados, mostrando un ajuste razonablemente óptimo entre la incidencia pronosticada y los datos de referencia reportados para la mayoría de los escenarios de ataque.

Estos resultados han permitido la comparación de la incidencia del conjunto de ataques *jamming* con brotes epidémicos de enfermedades conocidas.

CALIFICACIÓN DEL TRIBUNAL

Tesis Doctoral: *CARACTERIZACIÓN Y ANÁLISIS DE LA PROPAGACIÓN DE CIBERATAQUES JAMMING EN REDES DE SENSORES INALÁMBRICOS MEDIANTE MODELOS EPIDEMIOLÓGICOS.*

Autor: Miguel López Delgado.

Director y Tutor: Dr. Alberto Peinado Domínguez.

Director: Dr. Andrés Ortiz García.

El tribunal nombrado para juzgar la Tesis arriba indicada, compuesto por los siguientes doctores:

Presidente:

Vocales:

Secretario:

acuerdan otorgarle la calificación de:

Fdo.: _____

El Secretario del Tribunal

Fecha

En Málaga, a _____ de _____ de _____



UNIVERSIDAD
DE MÁLAGA

ÍNDICE DE CONTENIDOS

ÍNDICE DE CONTENIDOS	i
AGRADECIMIENTOS	v
CAPÍTULO 1. Introducción y Estado del Arte	1
1.1 Introducción	2
1.2 Justificación y relevancia de la Tesis	3
1.3 Propuesta de investigación y objetivos	6
1.4 Contribuciones	7
1.5 Estructura de la Tesis	9
1.6 Conclusiones	10
CAPÍTULO 2. Fundamentos sobre redes de sensores inalámbricos	11
2.1 Introducción	12
2.1.1 Arquitectura hardware típica de un nodo sensor	14
2.1.2 Elementos de software de un nodo sensor	16
2.1.3 Topologías de redes de sensores inalámbricos	20
2.1.4 Aplicaciones de las redes de sensores inalámbricos	23
2.1.5 Desafíos en el desarrollo e implementación de las redes de sensores inalámbricos	27
2.2 Protocolos de comunicaciones en redes	32
2.2.1 Modelos de referencia de arquitectura de protocolos	32
2.2.2 Protocolos de comunicación para redes de sensores inalámbricos	37
2.3 Conclusiones	47
CAPÍTULO 3. Fundamentos de Ciberseguridad en redes de sensores inalámbricos	49
3.1 Introducción	50
3.2 Clasificación de las amenazas y ataques contra redes de sensores inalámbricos	52
3.2.1 Amenazas y ataques según las características del atacante	53
3.2.2 Clasificación de ataques según la capa objetivo del protocolo OSI	56
3.3 Sistemas y mecanismos de seguridad ante ataques contra redes de sensores inalámbricos	66

3.3.1	Introducción	67
3.3.2	Mecanismos criptográficos	68
3.3.3	Protocolos de gestión de claves	70
3.3.4	Sistemas de gestión de confianza y autenticación	72
3.3.5	Sistemas de detección de intrusos	74
3.3.6	Otros mecanismos de seguridad	76
3.4	Ataques de interferencia contra redes de sensores inalámbricos	78
3.4.1	<i>Jamming</i> constante	80
3.4.2	<i>Jamming</i> engañoso	81
3.4.3	<i>Jamming</i> aleatorio	81
3.4.4	<i>Jamming</i> reactivo	82
3.4.5	Ataques <i>jamming</i> sofisticados	83
3.4.6	Descriptor estadísticos para la detección de ataques <i>jamming</i>	83
3.4	Conclusiones	85
CAPÍTULO 4. Fundamentos de la Teoría Epidemiológica		87
4.1	Introducción	89
4.2	Modelos epidemiológicos básicos	91
4.2.1	Modelos de enfermedades que no confieren inmunidad tras la infección	92
4.2.2	Modelos de enfermedades que confieren inmunidad tras la infección	94
4.3	Extensión de los modelos epidemiológicos básicos	98
4.3.1	Modelos epidemiológicos que contemplan tratamientos de la enfermedad	99
4.3.2	Modelos epidemiológicos que contemplan vectores de contagio	100
4.3.3	Modelos epidemiológicos que contemplan políticas de confinamiento	101
4.4	El modelo determinista Susceptible-Infectado-Recuperado	104
4.5	Introducción a los modelos epidémicos fenomenológicos	113
4.5.1	Modelos epidémicos de crecimiento exponencial y sub-exponencial	114
4.5.2	Modelos epidémicos de crecimiento logístico	115
4.6	Conclusiones	116

CAPÍTULO 5. Materiales y métodos	119
5.1 Introducción	120
5.2 El conjunto de datos	122
5.2.1 Modelos de ataques <i>jamming</i>	126
5.3 Pre-procesamiento de los datos	127
5.4 Modelado de la red de sensores inalámbricos	130
5.5 Definición de los grupos de individuos en la población de nodos sensores	133
5.6 Modelo SIR determinista para el estudio de la propagación de ataques <i>jamming</i>	136
5.7 Modelos <i>fenomenológicos</i> para el estudio de la propagación de ataques <i>jamming</i>	138
5.7.1 Modelo de Crecimiento Generalizado (GGM)	139
5.7.2 Modelo Generalizado de Crecimiento Logístico (GLGM)	139
5.8 Métodos de estimación y ajuste de parámetros	141
5.8.1 Ajuste de parámetros	141
5.8.2 Cuantificación los intervalos de confianza de parámetros	142
5.9 Conclusiones	144
CAPÍTULO 6. Estudio epidemiológico de la propagación de ataques <i>jamming</i>	
<i>jamming</i>	145
6.1 Introducción	146
6.2 Aplicación del modelo epidémico SIR determinista para la caracterización y análisis de la propagación de ataques <i>jamming</i>	148
6.2.1 Estudio retrospectivo de la propagación de ataques <i>jamming</i> mediante el modelo epidémico SIR determinista.	149
6.2.2 Estudio predictivo de la propagación de ataques <i>jamming</i> mediante el modelo epidémico SIR determinista	158
6.2.3 Análisis de resultados de la simulación de ataques <i>jamming</i> mediante el modelo epidémico SIR determinista	163
6.3 Aplicación del Modelo de Crecimiento Generalizado y del Modelo de Crecimiento Logístico Generalizado para la predicción de la propagación de ataques <i>jamming</i>	169
6.3.1 Estudio predictivo de la propagación de ataques <i>jamming</i> mediante el Modelo de Crecimiento Generalizado (GGM)	171
6.3.2 Estudio predictivo de la propagación de ataques <i>jamming</i> mediante el Modelo de Crecimiento Logístico Generalizado (GLGM)	175

6.3.3	Análisis de resultados de la simulación de los ataques <i>jamming</i> mediante Modelos de Crecimiento Generalizado	180
6.4	Conclusiones	185
CAPÍTULO 7. Conclusiones y trabajos futuros		187
7.1	Introducción	188
7.2	Conclusiones generales	188
7.3	Conclusiones particulares	190
7.4	Publicaciones relacionadas con la Tesis	192
7.5	Trabajos futuros	194
7.6	Conclusiones	195
APÉNDICE I		
Desarrollo de la Matriz de Siguiete Generación (<i>Next Generation Matrix</i>) para el cálculo del número reproductivo básico \mathcal{R}_0		197
APÉNDICE II		
Relación de tablas y datos relevantes obtenidos de los diferentes experimentos		201
APÉNDICE III		
Relación de figuras representativas obtenidas de los diferentes experimentos		215
REFERENCIAS		235

AGRADECIMIENTOS

Quiero agradecer, en primer lugar, la inestimable ayuda de mis directores de Tesis, los Doctores Alberto Peinado Domínguez y Andrés Ortiz García, destacando especialmente su paciencia y apoyo, además de la confianza depositada tanto en mí, como en mi propuesta de Tesis Doctoral, pues sin ellos ésta no hubiese sido posible.

También quiero agradecer, en segundo lugar, las facilidades que me han brindado en el uso de sus recursos e instalaciones el personal del departamento de Ingeniería de Comunicaciones. Esta ayuda ha sido clave para llevar a buen término el desarrollo de este trabajo y para la presentación y defensa de la Tesis. Agradecer también al personal responsable del Programa de Doctorado en Ingeniería de Telecomunicaciones por la admisión, apoyo y tramitación administrativa de esta Tesis Doctoral.

Por último, pero no menos importante, quiero agradecer también a mi familia y amigos, su paciencia y comprensión. Ellos saben bien quienes son y el por qué este agradecimiento.

A mi esposa Manuela, por ser un pilar fundamental en mi vida.

A mis hijos Manuel y Paula, para que el esfuerzo que he puesto en este trabajo les sirva como fuente de inspiración en sus vidas.

A mis padres, Ofelia y Asensio.

“Your time is limited, so don't waste it living someone else's life. Don't be trapped by dogma - which is living with the results of another people's thinking. Don't let the noise of other's opinions drown out your own inner voice. And most important, have the courage to follow your heart and intuition. They somehow already know what you truly want to become. Everything else is secondary.”

Steve Jobs.-

CAPÍTULO

1

Introducción y Estado del Arte

En los últimos años, la adopción de la tecnología de Redes de Sensores Inalámbricos (*Wireless Sensor Networks*, WSN) ha aumentado considerablemente, surgiendo nuevos paradigmas como la Industria 4.0 o el Internet de las Cosas (*Internet of Things*, IoT) entre otros. Sin embargo, debido factores como la naturaleza inalámbrica del canal, la reducida capacidad de procesamiento de los nodos, la dificultad de adoptar en todas las aplicaciones mecanismos de seguridad adecuados, o su despliegue en entornos desatendidos, entre otros, expone a estas redes a diversas amenazas desde el punto de vista de la Ciberseguridad, favoreciendo nuevas formas de ciberataques.

Por lo tanto, las redes de sensores inalámbricos han de afrontar cada vez retos más complejos desde el punto de vista de la Ciberseguridad, debiendo ser abordados introduciendo nuevas metodologías y modelos. En este sentido, la adopción de enfoques *bioinspirados*, los cuales se centran en comprender los fundamentos de ciertos sistemas biológicos, captando su comportamiento dinámico para ser posteriormente aplicado a sistemas no biológicos, ofrece un campo de estudio realmente interesante.

En este Capítulo se presenta una introducción a esta Tesis Doctoral, la cual se basa en la hipótesis de que la propagación de un determinado tipo de ciberataque contra una red de sensores inalámbricos, ha de seguir una dinámica de propagación similar al de la propagación dentro de una población de humanos, una enfermedad producida por un patógeno infeccioso o virus transmitido por el aire, tal como la gripe, el SARS o la COVID-19.

1.1 Introducción

El paralelismo entre el comportamiento de ciertas infecciones biológicas y algunos tipos de ciberataques en redes de comunicaciones, ha atraído a los investigadores en Ciberseguridad en los últimos años, llevando a éstos a aplicar modelos epidemiológicos para estudiar ciertos tipos de ataques contra redes de comunicaciones cableadas e inalámbricas. Desde entonces, se han desarrollado modelos epidemiológicos que han tratado de ajustarse a las características particulares de cada ataque, si bien la mayoría de ellos se centran en el análisis de la propagación de *malware*, lo que implica la necesidad de implementar código de programación o algoritmos para desplegar el ataque, algo que puede no ser posible debido a las limitaciones de los nodos inalámbricos. Sin embargo, existen otro tipo de ciberataques no basados en *malware* ni en programación compleja, que pueden ser ejecutados contra este tipo de redes independientemente de la complejidad de los nodos.

Esta Tesis Doctoral, iniciada en 2016, se basa en la hipótesis de que la propagación de un determinado tipo de ciberataque contra una red de sensores inalámbricos, ha de seguir una dinámica de propagación similar al de la propagación dentro de una población de humanos, de una enfermedad producida por un patógeno infeccioso o virus transmitido por el aire, tal como la gripe, el SARS o la COVID-19. El ciberataque a estudio será independiente de la complejidad y potencia de procesamiento de los dispositivos afectados, y para ello, se propone la utilización de los modelos matemáticos empleados en la Teoría Epidemiológica moderna, los cuales se emplean para estudiar y analizar la propagación de enfermedades infecciosas, buscando parones de comportamiento y midiendo su incidencia en una población objetivo.

Este enfoque de análisis de los ciberataques se enmarca en el concepto de sistemas *bioinspirados*, los cuales se centran comprender los fundamentos de ciertos sistemas biológicos, captando su comportamiento dinámico para ser posteriormente aplicado a sistemas no biológicos, ofreciendo un campo de estudio realmente interesante y, por su naturaleza, aplicable a las redes de sensores inalámbricos.

El principal objetivo de este enfoque es generar nuevas metodologías y modelos para diseñar, gestionar y asegurar sistemas no biológicos, y en especial, sistemas de redes de comunicaciones de naturaleza inalámbrica.

1.2 Justificación y relevancia de la Tesis

Como ya se ha comentado en la introducción, existe un paralelismo entre el comportamiento de la propagación de ciertas enfermedades infecciosas en una población, y la propagación de una infección por *malware* sobre los nodos de una red de comunicaciones [1]. Esto ha motivado a que se haya propuesto por parte de los investigadores en Ciberseguridad la aplicación de modelos epidemiológicos para estudiar ciertos tipos de ataques contra redes cableadas e inalámbricas, siendo en la mayoría de los casos, modelos que se centran en el análisis de la propagación de virus, gusanos informáticos y otro tipo de *malware*. El primer modelo de este tipo fue propuesto en 1991, y en él se estudiaba la propagación de un virus informático (*malware*) dentro de una red informática tradicional [2]. Desde entonces, estos modelos se han actualizado constantemente para describir la propagación de *malware* en diferentes tipos de redes, incluidas las redes de sensores inalámbricos. Como resultado, se han desarrollado modelos epidemiológicos que han tratado de ajustarse a las características particulares de cada ataque [3], [4], [5]. Por mencionar algunos de los artículos más interesantes, en [6] los autores propusieron un modelo epidemiológico que contemplaba la cuarentena (SIQRS), describiendo la dinámica de propagación de un gusano en una red inalámbrica, según un conjunto de individuos Susceptibles, Infectados, Cuarentena, Recuperados y nuevamente Susceptibles. Basado en este modelo, los autores estudiaron el equilibrio y la estabilidad del ataque en función de cada individuo, centrando su análisis en el Número Reproductivo Básico. En el trabajo presentado en [7] los autores propusieron un modelo no lineal de propagación de *malware* en redes de sensores inalámbricos, basado en el modelo epidemiológico clásico Susceptible, Infectado, Recuperado (SIR), mostrando que las características dinámicas de la propagación de *malware* están directamente relacionadas con el período de inmunidad de los nodos recuperados. Más recientemente, en [8] los autores propusieron un modelo epidemiológico para caracterizar la dinámica de propagación de más de una infección de código *malware* en una red de sensores inalámbricos. Su propuesta se basó en la variante del modelo Susceptible, Infectado, Recuperado y Susceptible, añadiendo la Vacunación (SIjRS-V). En [9], se presentó un estudio de la dinámica de propagación de gusanos en redes de sensores inalámbricos que se basaba en los cinco estados diferentes en los que los nodos se encontraban frente a la epidemia. A saber, Susceptibles, Expuestos, Infectados, Cuarentena y Recuperados

(SEIQR). El modelo propuesto demostraba el efecto del estado de cuarentena y recuperación en la propagación de virus tipo gusano en redes de sensores inalámbricos. En [10], los autores desarrollaron un modelo epidémico de ataque contra dispositivos IoT en el que, nodos internos y externos conseguían lanzar un ataque distribuido de denegación de servicio DDoS (*Distributed Denial of Service Attack*) basado en dispositivos IoT maliciosos que afectaban a los recursos específicos en la red objetivo. Este modelo se basaba principalmente en la *botnet* Mirai [11] hecha de dispositivos IoT y que se convirtió en el centro de atención con tres ataques DDoS importantes en 2016. En [12], se presentó un estudio donde se examinaba la efectividad del tratamiento de los dispositivos móviles según el tipo de infecciones de *malware* acumuladas. Este modelo consideraba seis clases de dispositivos móviles en función de su estado epidemiológico: Susceptibles, Expuestos, Infectados por *malware* hostil, Infectados por *malware* malicioso, en Cuarentena y Recuperados. En [13] los autores desarrollaron un modelo que constaba de cinco estados denominados Susceptible, Infeccioso, Cuarentena, Vacunado y Fallecido (SIQVD). La cuarentena se considera en este modelo un método a través del cual se puede detener la propagación de la infección en redes de sensores inalámbricos. Mientras que, con la vacunación se pretende eliminar el *malware* de la red. La combinación de técnicas de cuarentena y vacunación aportaba una mejora en la estabilidad de la red. Finalmente, en [14] los autores investigaron un modelo epidémico SEIQRS-V con tiempo de exposición para la propagación de códigos maliciosos en una red de sensores inalámbricos. En el modelo propuesto, se consideraron parámetros de interés como el radio de comunicación y la densidad de los nodos.

La mayoría de los trabajos descritos anteriormente, se centran en el análisis de la propagación de *malware* (virus y gusanos) lo que implica que para desplegar los ataques es preciso la implementación de código de programación o algoritmos de cierta complejidad. De acuerdo con el modelo de interconexión de sistemas abiertos OSI (*Open Systems Interconnection*), las capas superiores de este modelo son responsables de la traducción de datos entre servicios de red y aplicaciones, el intercambio continuo de información entre nodos, la transmisión de segmentos de datos entre puntos en una red, incluyendo segmentación, reconocimiento y multiplexación [15]. Esto implica que los ataques de virus, gusanos y, en general, de cualquier tipo de *malware* contra redes de sensores inalámbricos requiere utilizar las capas superiores de los dispositivos afectados (desde la capa de red hasta la capa de aplicación). Esto supone, además de la complejidad

ya mencionada, el uso extensivo de energía, memoria y capacidades de procesamiento de los nodos para realizar un ataque. Sin embargo, existen ciertos tipos de ciberataques, como el *jamming*, que pueden ejecutarse contra las capas inferiores (capa física y capa de acceso al medio) de un protocolo de comunicación. En este caso, el nodo atacante, por ejemplo, un nodo sensor manipulado, no necesitará un esfuerzo adicional para dañar la red, y podría, por tanto, utilizar varias estrategias con diferentes niveles de eficiencia, para llevar a cabo tales ataques contra las capas física y de acceso al medio, ya que esas capas son responsables de la primera etapa de la comunicación.

Por otro lado, en la mayoría de los trabajos anteriores no se establece una relación directa entre el número de nodos afectados y la propagación del ataque, sino que, por el contrario, se emplean métricas como la tasa de error de bits, el número de paquetes retransmitidos por los nodos afectados o el aumento de energía consumida por los nodos, entre otros. Conceptualmente, desde el punto de vista epidemiológico, este tipo de métricas no puede asociarse directamente con la propagación de un brote epidémico causado por una enfermedad.

Finalmente, con respecto a los escenarios presentados la mayoría de los modelos se apoyan en arquitecturas de red con nodos fijos, donde cada uno de ellos está conectado a un pequeño número de otros nodos a corta distancia.

En este sentido, la investigación presentada en esta Tesis Doctoral aporta una serie de aspectos diferenciadores y relevantes con respecto a los trabajos expuestos hasta ahora. Por una parte, se establece una relación directa entre el número de nodos afectados y la propagación del ataque, estando en consonancia con los conceptos presentados en epidemiología. Esto permite además no sólo tratar el ataque desde el punto de vista retrospectivo o a posteriori, sino que permite implementar modelos que proporcionan una visión predictiva o pronóstico a corto y medio plazo de la propagación del ataque. Por otra parte, el ciberataque a estudio es independiente de la complejidad y potencia de procesamiento de los dispositivos afectados, por lo que el modelo epidémico propuesto considera el estudio de los ataques de *jamming* como un medio de propagación de la epidemia. Finalmente, con respecto a los escenarios de estudio, la experimentación se ha realizado sobre diferentes tipos de ataques *jamming* y tres escenarios diferentes, apoyados en una arquitectura de red con nodos fijos, donde cada uno de ellos está conectado a un número suficiente de nodos como para obtener resultados significativos en cuanto a los efectos de la propagación del ataque.

1.3 Propuesta de investigación y objetivos

En esta Tesis Doctoral se propone la caracterización y análisis de la propagación de ataques *jamming* en redes de sensores inalámbricos mediante la aplicación de modelos epidemiológicos. Este enfoque se enmarca en el concepto de sistemas *bioinspirados* [16], los cuales se centran comprender comportamiento dinámico de ciertos sistemas biológicos, para ser posteriormente aplicado a sistemas no biológicos.

Como se verá posteriormente, existen una gran variedad de amenazas y ataques contra redes de sensores inalámbricos que pueden degradar su funcionalidad no solo en aplicaciones ya implementadas, sino también en nuevos paradigmas emergentes que tienden a consolidarse tales como la Industria 4.0 o la Internet de las Cosas (*Internet of Things*, IoT) entre otros. En este contexto, la utilización de modelos biológicos que expliquen la dinámica de transmisión de patógenos, proporciona un medio para evaluar estas amenazas y por su naturaleza, aplicable a las redes de sensores inalámbricos.

La hipótesis central en la que se basa esta Tesis Doctoral, es que, la propagación de un determinado tipo de ciberataque contra una red de sensores inalámbricos, ha de seguir una dinámica de propagación similar al de la propagación dentro de una población de humanos, de una enfermedad producida por un patógeno infeccioso o virus transmitido por el aire. Para ello, se propone la utilización de los modelos matemáticos empleados en la Teoría Epidemiológica moderna, los cuales se emplean para estudiar y analizar la propagación de enfermedades infecciosas, buscando parones de comportamiento y midiendo su incidencia en una población objetivo.

El ciberataque a estudio es independiente de la complejidad y potencia de procesamiento de los dispositivos afectados, por lo el modelo epidémico propuesto considera el estudio de los ataques de *jamming* (tradicionalmente conocidos como ataques de interferencia). Este tipo de ciberataque, no está basado en *malware* o programación compleja, por lo que puede lanzarse para dañar una red de sensores inalámbricos, independientemente de la capacidad de los nodos que se usen para ejecutarlo.

El objetivo principal de esta Tesis Doctoral es diseñar, desarrollar y proponer nuevas metodologías y modelos que permitan mejorar la Ciberseguridad de las redes de sensores inalámbricos y reducir así el riesgo asociado a un ciberataque en este tipo de redes, bien reduciendo el factor de probabilidad de riesgo, reduciendo el factor de impacto, o ambos a la vez.

1.4 Contribuciones

Las publicaciones que han surgido a raíz del desarrollo de la presente Tesis, cubren dos campos de estudio bien diferenciados. Por una parte, se han publicado una serie de artículos basado en sistemas *bioinspirados*, relacionados con la Ciberseguridad en redes de sensores inalámbricos propiamente dicha, donde se han tratado los ataques *jamming* contra este tipo de redes como brotes epidémicos [17], [18], [19], [20], [21]. En este mismo grupo de artículos sobre sistemas *bioinspirados*, se incluye un modelo para detección de intrusos basado en la Teoría de Juegos Evolutiva [22]. Por otra parte, y motivado por la investigación en el campo de la epidemiología, se ha publicado un trabajo de investigación relevante donde se abordó la propagación de la segunda ola de la pandemia de COVID-19 en el territorio español [23].

Al inicio de esta investigación, se propuso el modelo SEIS (Susceptible, Expuesto, Infectado y Susceptible), como modelo epidémico de referencia para la caracterización de la propagación de ataques *jamming* [17], [18], [19]. En estos artículos se estudiaba el número reproductivo básico, como uno de los factores más importantes pues éste determinará si la epidemia (ataque) se propagará o no entre los nodos de la red inalámbrica. Además de se llevaron a cabo una serie de simulaciones para explicar los resultados y analizar el equilibrio y la estabilidad de las soluciones encontradas. Sin embargo, tras realizar los primeros experimentos utilizando datos de referencia de ataques *jamming*, se comprobó que el comportamiento dinámico de la red ante este tipo de ataques se asemejaba más a un modelo epidemiológico *Susceptible, Infectado Recuperado* (SIR). Estos resultados se validaron inicialmente en [20], donde se observó por una parte que, debido a la velocidad con la que se producen las transmisiones dentro de la red, no tenía sentido contemplar un tiempo o periodo de latencia para los nodos expuestos, ya que este tiempo sería prácticamente inapreciable con respecto a parámetros como la tasa de contagio o el tiempo de recuperación. Por otro lado, también se observó que, dado que los nodos incorporan protocolos de enrutamiento en capas superiores, éstos actúan de algún modo como un sistema inmunológico, permitiendo recuperar la comunicación a través rutas alternativas. Así, una vez que los nodos establecen esas nuevas rutas, y siempre que sea posible, permanecerán en el grupo de los recuperados, ya que no estarán afectados por el ataque y además no soerán propagadores de éste. Tal situación debería mantenerse, al menos, mientras no se produzca un ataque en otra zona de la red, o

mientras no se provoque un tipo diferente de ataque. Este hecho se contrastó en un artículo en el que se validaba de forma extensiva los resultados experimentales obtenidos hasta la fecha [21]. Para ello se consideró el modelo epidemiológico determinista Susceptible, Infectado, Recuperado (SIR), y se analizaron los resultados de una serie de simulaciones, contrastándolas con un conjunto de datos de referencia [22]. Aquí, el término *jamming* se consideró tanto desde el enfoque más clásico de señales de interferencia, centrándose en el nivel físico de los sistemas, como en el enfoque de Ciberseguridad que incluye los ataques generados en capas superiores de la pila de protocolos OSI, principalmente en la capa física y la capa de acceso al medio, produciendo el mismo efecto en el canal de comunicación. Este artículo se considera de especial relevancia en el desarrollo de esta Tesis Doctoral.

Por otra parte, en este mismo contexto de modelos *bioinspirados*, también se desarrolló un artículo donde se propuso un mecanismo de detección de intrusos (*Intrusion Detection System*, IDS) para identificar nodos maliciosos en redes de sensores inalámbricos [23]. Aquí, las interacciones entre los nodos maliciosos y los nodos que actúan como IDS se modelaron como un juego evolutivo basado en la suposición de que ambos jugadores tenían una racionalidad limitada y un razonamiento estratégico acotado. Los resultados analíticos demostraron que es posible lograr la estrategia de detección más efectiva durante el juego si la población de IDS sigue la estrategia evolutivamente estable. Finalmente, los resultados de la simulación demostraron que, al establecer los parámetros de configuración adecuados, el modelo diseñado puede detectar de manera efectiva los nodos maliciosos, al mismo tiempo que mejora el uso de los recursos.

Por último, la investigación llevada a cabo en esta Tesis Doctoral en el campo de la epidemiología, y lamentablemente el entorno de pandemia en el que ésta se ha desarrollado, motivó que se propusiese la publicación de un trabajo de investigación relevante donde se abordase la propagación de la pandemia de COVID-19. Fruto de esta motivación se publicó un artículo donde se caracterizó la evolución de la segunda ola de la epidemia de COVID-19 en España, usando un modelo epidemiológico de tipo *fenomenológico* [24]. En este artículo el estudio se llevó a cabo utilizando un enfoque epidémico de dos pasos. Primero, se utilizó un modelo de crecimiento generalizado simple para ajustar los parámetros principales en la fase epidémica temprana de cada ola. Posteriormente, se aplicaron los resultados obtenidos sobre un modelo de crecimiento logístico para caracterizar completamente ambas olas. Los resultados demostraron que

incluso en ausencia de series de datos precisas, los modelos propuestos permitieron caracterizar las curvas de incidencia de casos, e incluso elaborar pronósticos a corto plazo. De hecho, en este mismo trabajo, se realizó una predicción de la evolución de la incidencia en un horizonte temporal de 60 días vista obteniendo resultados que, lamentablemente, posteriormente se comprobaron que eran bastante acertados.

Cabe señalar en este punto que, en el momento de redactar esta Memoria de Tesis Doctoral, se está desarrollando un artículo (aún sin publicar) relacionado con la aplicación de modelos epidemiológicos de tipo *fenomenológico* para pronosticar la propagación de ataques *jamming* en redes de sensores inalámbricos, a partir de los datos iniciales del ataque. Este tipo de modelos epidemiológicos, que se describirán con más detalle a lo largo de los capítulos correspondientes, enfatizan en la reproducibilidad de las observaciones empíricas utilizando modelos simples, sin una base específica sobre las leyes o los mecanismos físicos que dan lugar a los patrones observados en los datos. Hasta donde se ha podido constatar, no existen hasta la fecha propuestas de investigación que apliquen los modelos epidemiológicos de tipo *fenomenológico* a la predicción, análisis y evaluación de la propagación de ciberataques en redes de sensores inalámbricos. Este enfoque supone, por tanto, una contribución relevante de esta Tesis Doctoral en el campo de la Ciberseguridad.

1.5 Estructura de la Tesis

El resto de la Memoria de Tesis Doctoral se organiza como sigue. En el Capítulo 2 se ofrece una revisión del estado actual del arte en cuanto a la tecnología de redes de sensores inalámbricos. En el Capítulo 3 se abordan los aspectos principales relacionados con la Ciberseguridad en redes de sensores inalámbricos, aportando una visión de conjunto sobre las principales amenazas y ataques, así como de los mecanismos y sistemas de seguridad que habitualmente se implementan en este tipo de redes. En el Capítulo 4 se presenta un estudio de los modelos matemáticos más relevantes utilizados en epidemiología. Dentro de este amplio campo de estudio, se definen en primer lugar los conceptos básicos propios de la epidemiología, para posteriormente continuar con una descripción los modelos epidemiológicos *mecanicistas*, y los modelos epidemiológicos *fenomenológicos*. En el Capítulo 5 se describen los materiales y métodos utilizados para el desarrollo de los experimentos para la validación de los modelos epidemiológicos

propuestos. Aquí se ha realizado una descripción detallada del modelo de red de sensores inalámbricos a estudio, definiendo aspectos como la estructura de la red sobre la que se propagará el ataque *jamming* y los protocolos utilizados. En este mismo Capítulo se describen los modelos epidemiológicos que se utilizarán para el desarrollo de los experimentos y simulaciones, el modelo SIR determinista, al que se le añade el grupo de los nodos caídos, y los modelos de crecimiento generalizado (GGM) y de crecimiento logístico generalizado (GLGM) respectivamente. En el Capítulo 6, y como contribución principal de esta Tesis Doctoral, se ha realizado la validación experimental de los modelos propuestos para el desarrollo de esta investigación, mediante la elaboración de un estudio epidemiológico donde, a través de un conjunto de experimentos y simulaciones, se caracterizan y analizan los ataques *jamming* de tipo aleatorio y reactivo, llevados a cabo contra una red de sensores inalámbricos objetivo. El análisis de los resultados obtenidos se presenta también en este Capítulo. Finalmente, en el Capítulo 7 se exponen las principales conclusiones extraídas de esta investigación en la que se ha presentado un enfoque epidemiológico de propagación de enfermedades, para la caracterización y análisis de los ataques tipo *jamming* en redes de sensores inalámbricos. Con el fin de no extender en exceso alguno de los capítulos mencionados, se ha incluido un apartado con varios Apéndices. En el Apéndice I se presenta el desarrollo de la Matriz de Siguiete Generación (*Next Generation Matrix*) utilizada para el cálculo del número reproductivo básico \mathcal{R}_0 . El Apéndice II conjunto de datos en forma de tablas utilizados como referencia, así como los resultados obtenidos de los experimentos objeto de la investigación. Finalmente, el Apéndice III los gráficos y figuras igualmente obtenidas de los experimentos y simulaciones.

1.6 Conclusiones

En este Capítulo se ha presentado una introducción a la Tesis, mencionando los aspectos más relevantes de ésta, incidiendo en el paralelismo entre el comportamiento de ciertas infecciones biológicas y los ciberataques en redes de sensores inalámbricos. También se han destacado los aspectos diferenciadores y relevantes propuestos en esta Tesis, así como las principales contribuciones.

En lo que sigue, se desarrollarán el resto de Capítulos tal y como se indica en el apartado de estructura del documento.

CAPÍTULO

2

Fundamentos sobre redes de sensores inalámbricos

Las Redes de Sensores Inalámbricos (*Wireless Sensor Networks*, WSN) consisten en un gran número de pequeños dispositivos denominados nodos que se despliegan de forma extensiva en un determinado entorno para realizar tareas de monitorización, automatización, seguridad, control y en general cualquier otra aplicación que requiera la recopilación de datos en tiempo real. Estas redes se basan en la cooperación entre nodos para crear rutas de comunicación inalámbricas, y junto con su carácter escalable, proporcionan un mejor desempeño en aquellas aplicaciones en las que las redes cableadas tradicionales son imposibles de desplegar o resultan muy costosas.

En este Capítulo se proporciona una visión general de los fundamentos relativos a redes de sensores inalámbricos, incluyendo aspectos como los elementos hardware y software que componen los nodos, así como las arquitecturas y protocolos de red sobre las que se sustenta esta tecnología.

2.1 Introducción

De forma general, tal y como se representa en la Figura 2.1, una red de sensores inalámbricos (*Wireless Sensors Networks*, WSN) puede definirse en su modo más simple como una red de dispositivos, habitualmente de pequeño tamaño y baja complejidad denominados *nodos* o *motas*, que pueden detectar el entorno y comunicar la información recopilada a través de enlaces o canales inalámbricos, de modo que los datos son reenviados mediante retransmisión a través de múltiples saltos usando otros nodos, hasta llevar esa información a uno o varios nodos recolectores llamados nodos de agregación o coordinadores de red, que pueden usar estos datos localmente o reenviarlos nuevamente otras redes como por ejemplo, una red corporativa o Internet [25].

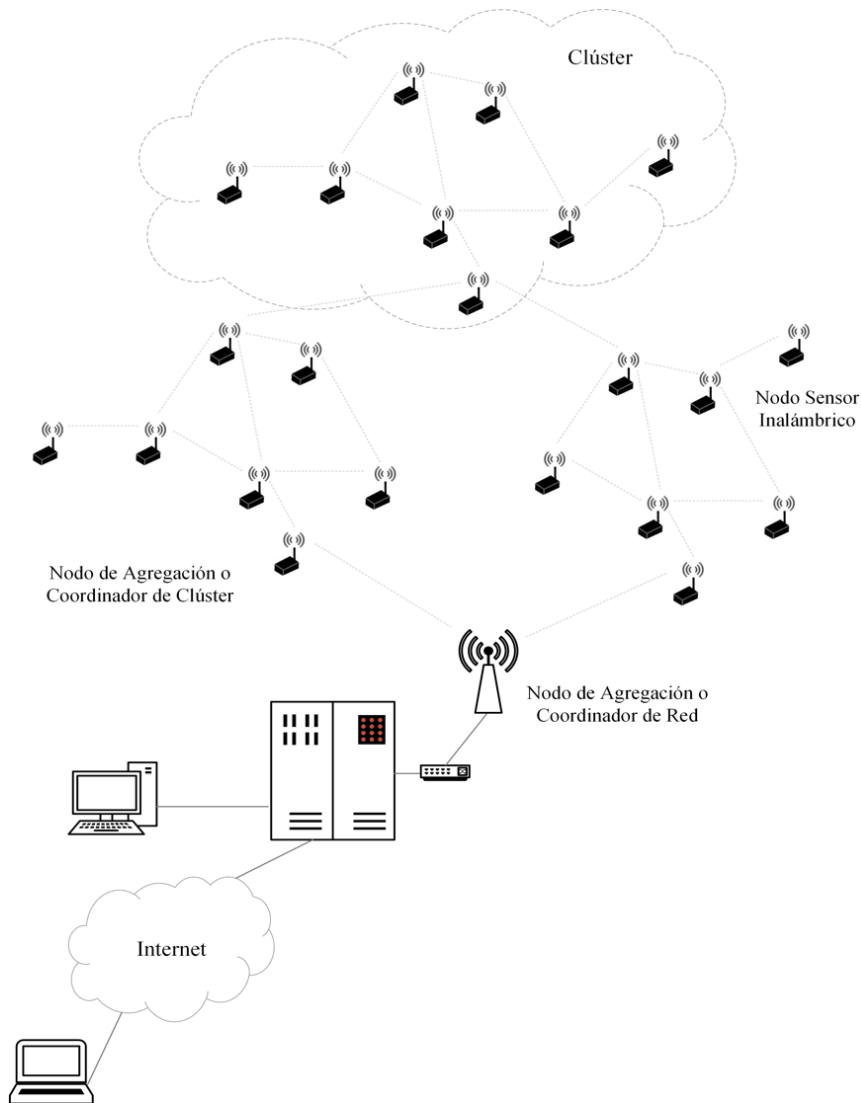


Figura 2.1. Red de Sensores Inalámbricos (*Wireless Sensor Network*, WSN).

El término red de sensores inalámbricos se emplea, por tanto, para referirse a un sistema heterogéneo que combina cientos de pequeños nodos sensores y actuadores de bajo coste y bajo consumo de energía con capacidades de computación reducidas, junto con otros dispositivos de mayores prestaciones. Estas redes habitualmente se despliegan de forma fija en el entorno que se quiere monitorizar o sobre el que se quiere actuar, si bien en ciertas aplicaciones, puede recurrirse a nodos móviles.

Para llevar a cabo las tareas de computación y comunicación de los datos recopilados, los nodos sensores se equipan con hardware y software específico representados de forma simplificada en el esquema de la Figura 2.2. Debido a las limitaciones en tamaño, capacidad de procesamiento y alimentación de los nodos sensores, todos estos elementos se diseñan con técnicas que les permitan aprovechar al máximo los recursos disponibles y minimizar el consumo de energía, utilizando para ello sistemas integrados (*embedded systems*).

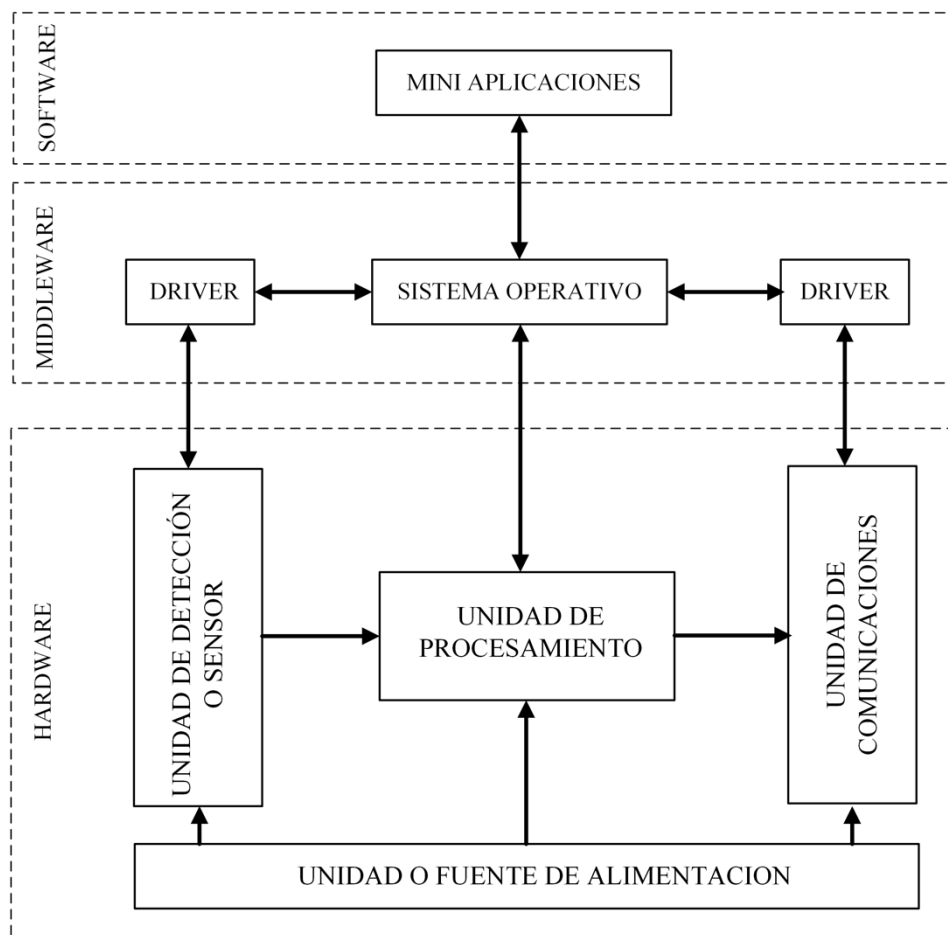


Figura 2.2. Esquema simplificado del hardware y software de un nodo sensor.

Por otra parte, tecnologías emergentes como el Internet de las cosas (IoT, *Internet of Things*), también hacen uso de las funcionalidades que aportan las redes de sensores inalámbricos. Básicamente, una red IoT es la tecnología más moderna mediante la cual un sistema se controla localmente y también globalmente a través de Internet. Estas nuevas redes se componen de objetos inteligentes que interactúan con otros objetos inteligentes heterogéneos, siendo direccionables de forma única en función de los protocolos de comunicación estándar [26]. Las redes IoT requieren, por tanto, de plataformas que sean capaces de cumplir estos nuevos requisitos en cuanto al acceso y control de los dispositivos que conforman la red de forma transparente, y a la vez minimizando el consumo de recursos. En este sentido, las redes IoT han sido capaces de explotar todos los avances aportados por las redes de sensores inalámbricos tradicionales.

2.1.1 Arquitectura hardware típica de un nodo sensor

Desde el punto de vista del hardware, pueden distinguirse varias arquitecturas, entre las que destacan las basadas en microcontroladores (*Micro Controller Unit*, MCU), las basadas en los procesadores digitales de señales (*Digital Signal Processor*, DSP), las basadas en circuitos integrados programables (*Field-Programmable Gate Array*, FPGA *System on Programmable Chips*, SoPC), o las basadas en circuitos integrados de aplicación específica (*Application Specific Integrated Circuit*, ASICs) [27], o *Advanced Microcontroller Bus Architecture* (AMBA) [26] entre otras. A modo de ejemplo, en la Figura 2.3 se representa el hardware básico que incorpora un nodo típico basado en la arquitectura MCU. Si bien este tipo de nodos tienen recursos limitados en términos de capacidad de memoria y procesamiento, en la actualidad la arquitectura MCU sigue siendo una de las más utilizada ya que junto a su bajo coste, proporciona una alta flexibilidad, bajo consumo de energía y facilidad de uso y mantenimiento. En esta arquitectura se distinguen cuatro elementos principales: la unidad de detección o muestreo con su correspondiente conversor analógico/digital (*Analogic to Digital Converter*, ADC); la unidad de procesamiento, compuesta por un microcontrolador y unidades de memoria; la unidad de comunicaciones vía radio y la unidad o fuente de alimentación. De forma adicional la placa del sensor puede incluir actuadores con el exterior y/o contener elementos de localización (GPS).

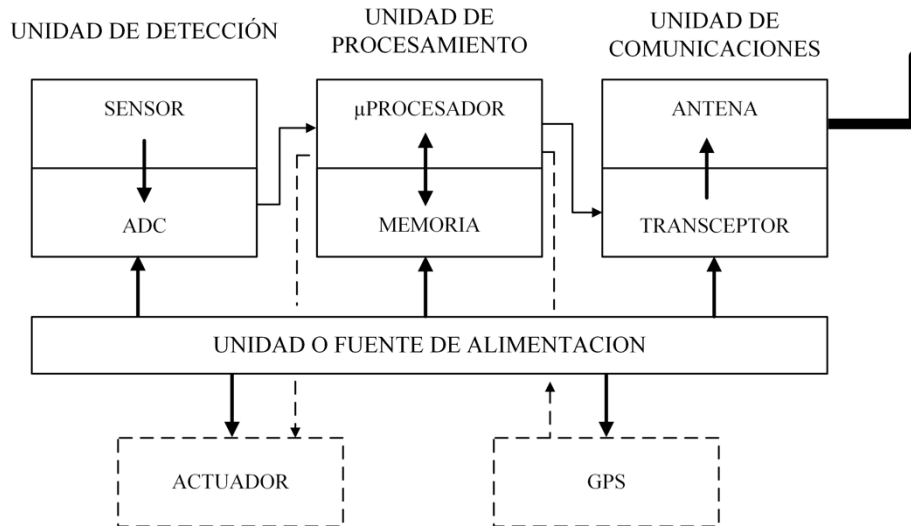


Figura 2.3. Arquitectura hardware básica de un nodo sensor basado en MCU.

La unidad de detección puede considerarse el componente principal de una red de sensores y está formada por el sensor propiamente dicho, cuya función es recopilar la información del entorno y por un módulo ADC encargado de convertir esta información a formato digital para su posterior procesamiento. La placa del sensor puede contener diferentes tipos de elementos de detección que van desde sensores magnéticos de baja velocidad de muestreo hasta sensores térmicos, visuales, infrarrojos, acústicos o de radar. La unidad de procesamiento integrada es el núcleo del nodo sensor, y se compone un micro procesador, cuya función principal es programar tareas, procesar datos y controlar la funcionalidad de otros componentes de hardware, y una serie de unidades de memoria. La memoria volátil tipo RAM se utiliza para almacenar las lecturas del sensor, almacenar datos intermedios, o paquetes de datos recibidos de otros nodos; mientras que las memorias no volátiles tipo EEPROM y FLASH están dedicadas a almacenar el código de los programas o cualquier otra información que ha de quedar de forma permanente en el dispositivo. La unidad de comunicaciones tiene la función de establecer los enlaces por radiofrecuencia (RF) entre los nodos de la red de sensores. Generalmente está formada por un módulo transceptor, encargado de acondicionar los datos transmitidos y recibidos (modulación, filtrado, multiplexación/demultiplexación, etc.), y una antena de baja potencia de salida (0 dBm o 1 mW típico) que opera en la banda industrial, científica y médica (*Industrial, Scientific and Medical band, ISM*) con frecuencias que oscilan entre los 433 MHz y 2.4 GHz y con un alcance que puede variar entre los 10 y los 150 m, dependiendo de la tecnología de radio frecuencia y modulación empleadas [27]. Por

último, la unidad o fuente de alimentación es la encargada de suministrar suministra energía necesaria a los componentes del nodo sensor, tales como la unidad detección, la unidad de procesamiento, la unidad de comunicación y a cualquier otro elemento hardware que incorpore el nodo, siendo por lo tanto un componente fundamental. Las baterías son la principal fuente de alimentación de los nodos sensores, y aunque habitualmente éstas tienen una capacidad limitada, existen alternativas como el uso de energía solar que permite su recarga y extender la vida útil de éstas. Por lo tanto, minimizar el consumo de energía siempre es un objetivo clave tanto en el diseño de los nodos sensores, como en la operativa habitual de las redes de sensores.

Como ejemplo, un nodo típico *Mica2 mote* se compone de un microcontrolador ATmega128L, con 4 Kb de memoria RAM estática y 128 Kb de memoria flash para el programa. Además, incorpora dos tipos de transceptores de RF, el *Chipcon CC1000* y el *RFM TR1000*, proporcionando un rango de transmisión de alrededor de 150 m [28].

2.1.2 Elementos de software de un nodo sensor

Las tareas de computación y comunicación de la información de los nodos sensores son realizadas por un conjunto de elementos software cuya característica principal es el estar especialmente diseñados para poder ejecutarse en este tipo de dispositivos. En la Figura 2.4 se representa un esquema de una serie de módulos de software básicos que pueden encontrarse en un nodo sensor.

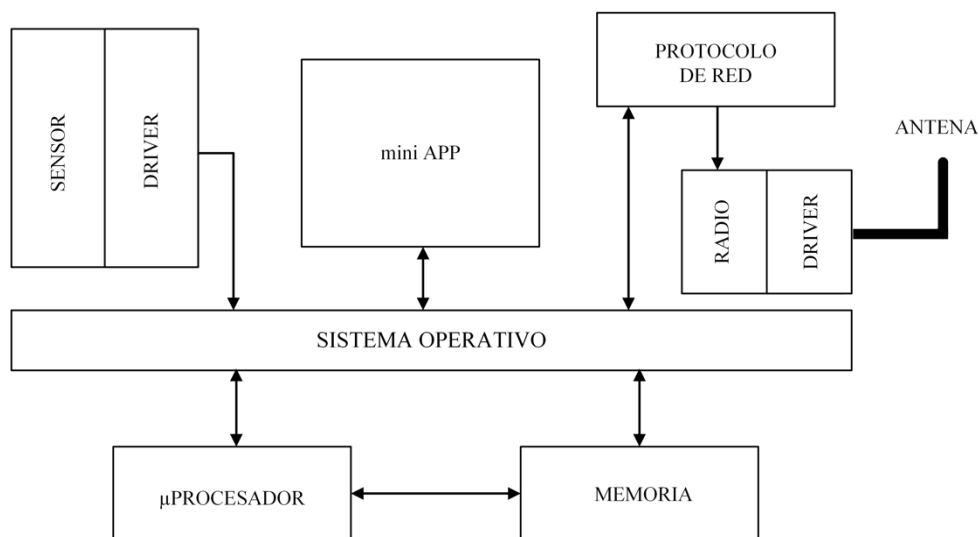


Figura 2.4. Módulos software básicos de un nodo sensor.

Cómo núcleo principal del software, se dispone del Sistema Operativo, el cual contiene el *microcódigo* o *middleware* utilizado para interactuar con el resto de módulos de software de alto nivel, proporcionando el interfaz de comunicación entre las aplicaciones, los controladores y el hardware. Para aprovechar las capacidades de los nodos, y especialmente para hacer frente a sus limitaciones ya comentadas en cuanto a capacidad de procesamiento y almacenamiento, así como la necesidad del uso eficiente de la fuente de alimentación es necesario utilizar sistemas operativos ligeros. Esto hace que los sistemas operativos tradicionales no sean capaces de satisfacer estos requisitos, por lo que se emplean sistemas operativos alternativos específicos para este tipo de dispositivos. Por otra parte, debido a la variedad de hardware que incorporan los nodos, los sistemas operativos han de ser capaces, a su vez, de ejecutarse sobre una amplia gama de plataformas, ya sean basadas en microcontroladores (MCU), en procesadores digitales de señales (DSP), en circuitos integrados programables (FPGA, SoPC), o en circuitos integrados de aplicación específica (ASICs) y todos ellos con diferentes capacidades de procesamiento (por ejemplo, de 8 a 32 bits) y diferentes tipos y capacidad de almacenamiento como memoria RAM, EEPROM y FLASH [27].

Uno de los sistemas operativos más extendidos en el mundo de las redes de sensores inalámbricos es TinyOS. Se trata de sistema operativo de código abierto y basado en eventos, desarrollado originalmente por la Universidad de California, Berkeley, y que actualmente dispone de una amplia comunidad de usuarios y desarrolladores lo que lo ha convertido en un sistema operativo estándar para redes de sensores inalámbricos, ya sea en el campo de la investigación, como en aplicaciones comerciales. TinyOS está escrito en lenguaje NesC (*Network Embedded Systems C*) es una adaptación del lenguaje de programación C, optimizada para las limitaciones de memoria, potencia de procesamiento de las redes de sensores. TinyOS admite microprocesadores que van desde arquitecturas de 8 bits con tan solo 2 KB de RAM a procesadores de 32 bits con 32 MB de RAM o más. Este sistema operativo proporciona un conjunto de interfaces de programación de aplicaciones (*Application Programming Interface, API*) para la programación de mini aplicaciones [29].

A parte de TinyOS, existen otros sistemas operativos que actualmente están teniendo un papel importante en el desarrollo e implementación de aplicaciones para redes de sensores inalámbricos y, en especial, tras al auge de las aplicaciones relacionadas con el *Internet de las cosas*, (*Internet of Things, IoT*). Es el caso de *Contiki*, un sistema

operativo muy ligero basado en un núcleo (*kernel*) controlado por eventos, que a su vez proporciona la ejecución de múltiples subprocesos. *Contiki* está implementado en lenguaje C y ha sido adaptado a varias arquitecturas de microcontroladores, incluyendo la familia Texas Instruments MSP430 o Atmel AVR [30]. Otro sistema operativo de amplia implementación es RIOT OS, un sistema operativo cuyos objetivos de diseño son la eficiencia energética, reducido uso de memoria, modularidad y acceso uniforme a las interfaces de las aplicaciones, independiente del hardware sobre el que se implemente. RIOT OS se considera, por tanto, diseñado explícitamente para dispositivos con recursos mínimos, pero facilita a su vez, el desarrollo de aplicaciones en una amplia gama de dispositivos. Para ello RIOT OS permite la programación estándar en C y C ++, proporciona múltiples subprocesos, así como capacidades en tiempo real, y solo necesita un mínimo de 1,5 kB de RAM [31].

Finalmente, también se han hecho intentos por implementar en los nodos sensores sistemas operativos que originalmente se desarrollaron para dispositivos móviles como los *Smartphone*. Entre ellos destaca *Brillo* (también llamado *Android Things*) que es una versión optimizada de Android para dispositivos con recursos limitados tales como los nodos empleados en las redes de sensores inalámbricos. Este sistema operativo, fue lanzado por Google en 2015 y actualmente dispone de una amplia comunidad de desarrolladores [32]. *Brillo* permite la programación de aplicaciones para dispositivos sensores disponiendo además de las herramientas de desarrollo y los recursos propios Android, de una serie de API que proporcionan interfaces de entrada y salida (E/S) de bajo nivel y librerías de controladores para los componentes habitualmente utilizados en los nodos, como sensores de temperatura, movimiento, etc.

Continuando con los elementos de software que se implementan en un nodo sensor, los controladores o *drivers* son módulos de software encargados de gestionar las funciones básicas de los componentes hardware del nodo, permitiéndoles interactuar con otros elementos de hardware o ser utilizados por las mini-aplicaciones a través del sistema operativo. Tal y como se ha comentado, estos *drivers* suelen desarrollarse junto con el sistema operativo a modo librerías para diferentes tipos de hardware ya sean microcontroladores, transceptores, módulos de detección y captación, interfaces de radio, etc. Estos *drivers* deben encapsular las secuencias requeridas para la manipulación del hardware de bajo nivel y permitir la activación las funcionalidades solicitadas. Las especificaciones de estas secuencias se describen generalmente en hojas de datos

proporcionadas por el fabricante del hardware, siendo vital asegurar que estas propiedades funcionales se conserven siempre durante el tiempo de ejecución [29].

Por otra parte, el módulo de software que contiene la implementación de la pila del protocolo de red es el encargado de gestionar las funciones básicas de la comunicación inalámbrica entre los nodos. Este módulo interactúa estrechamente con los *drivers* del dispositivo para intercambiar paquetes de datos con otros nodos. De forma general, la pila de protocolo se implementa a modo de bloques que contienen las distintas capas del protocolo de red. Aunque estas capas serán descritas posteriormente con mayor detalle, la implementación contempla, al menos, la capa de abstracción de hardware incluyendo la capa física, la capa de acceso al medio o MAC (*Medium Access Control*), y una capa de red. Entre otras, las funciones que desempeña este módulo son el enrutamiento de paquetes de datos, mantenimiento de la topología de red, control de acceso medio, mecanismos de cifrado, mantenimiento de la calidad de la señal de los enlaces de comunicación etc. A modo de ejemplo, uno de los chips de comunicaciones más ampliamente utilizados en nodos sensores es el TI CC2420 [33]. Se trata de un transceptor que trabaja en la banda de 2.4 GHz e incorpora las capas física y MAC del protocolo IEEE 802.15.4, si bien el resto de las funcionalidades y capas de la pila de protocolos que se deseen utilizar han de implementarse mediante software.

Finalmente, para aprovechar las capacidades de los nodos éstos se programan con una serie de *mini-APP* (aplicaciones básicas) las cuales acceden a las funcionalidades de los distintos módulos que lo componen, permitiendo, por ejemplo, el pre-procesamiento de los datos, la conversión analógica a digital y viceversa, el almacenamiento de datos, la realización de cálculos, etc. Estas aplicaciones deben desarrollarse de modo que permitan hacer frente las limitaciones de estos dispositivos en cuanto a capacidad de procesamiento y almacenamiento, así como la necesidad del uso eficiente de la fuente de alimentación. Como ejemplo, en el grupo de desarrolladores de Brillo, el usuario puede encontrar información para crear aplicaciones utilizando el entorno de programación Android Studio 3.1 y alguna de las placas hardware compatibles con *Android Things* (NXP Pico i.MX7D y *Raspberry Pi 3 Model B*). Con este modelo de programación el usuario no precisa desarrollar el núcleo (*kernel*) o firmware ya que es el propio Google quien gestiona el paquete de soporte de toda la plataforma de desarrollo, ya que las imágenes de software con actualizaciones y correcciones se crean y se envían a los dispositivos a través de *Android Things*. Así mismo, existe hardware comercial basado en

microcontroladores que dispone de las funcionalidades requeridas para desarrollar dispositivos IoT. En este sentido, *Arduino* y *Raspberry Pi* son las plataformas más populares. La primera incluye transceptores WIFI y Bluetooth integrados, además permite utilizar Entrada/Salida de propósito general (GPIO, *General Purpose Input/Output*), y bus serie universal (USB, *Universal Serial Bus*), para conectar diferentes dispositivos externos. El entorno de desarrollo integrado o IDE (*Integrated Development Environment*), incluye lenguajes de programación como Python, Java entre otros [26].

2.1.3 Topologías de redes de sensores inalámbricos

La topología de la red de sensores inalámbricos, también conocida como estructura de red, define el modo en el que se disponen los nodos sensores en un área de detección determinada. El despliegue de una red de sensores inalámbricos puede realizarse, por tanto, utilizando diferentes topologías, las cuales dependen de múltiples factores que abarcan desde la propia aplicación de la red, la necesidad de movilidad de los nodos, hasta la capacidad de comunicación y procesamiento de los nodos, o los protocolos de comunicaciones utilizados. En este sentido, y para el desarrollo de esta Tesis, se asume que las redes objeto del ataque son redes estáticas bidimensionales, que adoptan alguna de las topologías de red básicas descritas a continuación.

Un aspecto importante de las redes de sensores inalámbricos es el concepto de agregación de datos, cuyo objetivo es reducir el número de mensajes enviados a través de la red, conservando la energía de los nodos y aumentando su área de cobertura. Básicamente, la agregación de datos consiste en enviar los datos captados por varios nodos sensores ubicados en una determinada zona, hasta otro nodo concreto, llamado nodo de agregación o coordinador de red, donde los datos son agrupados y reenviados nuevamente a otro punto de la red. Los nodos de agregación pueden hacer, a su vez, de puentes de conexión (*Gateway*), entre la red de sensores y otras redes (WIFI, 5G, satélite, etc.), permitiendo el envío de información desde la zona de despliegue de la red de sensores, a centros de proceso, o permitiendo ser la interfaz entre el usuario y la red de sensores. Los nodos de agregación pueden ser dispositivos iguales que los nodos sensores en cuanto a capacidad de procesamiento o transmisión, pero en el caso de actuar como *Gateway* entre redes, estos nodos suelen ser más potentes, disponiendo de mayor capacidad de

almacenamiento y procesamiento, e incorporando diferentes interfaces de comunicaciones (WIFI, 4G, Ethernet, etc.).

A modo de ejemplo, en la Figura 2.5 se representan tres topologías típicas utilizadas en el despliegue de redes de sensores inalámbricos. En ellas, los nodos sensores crean enlaces radio para enviar a otro nodo de la red la información que ellos mismos recopilan.

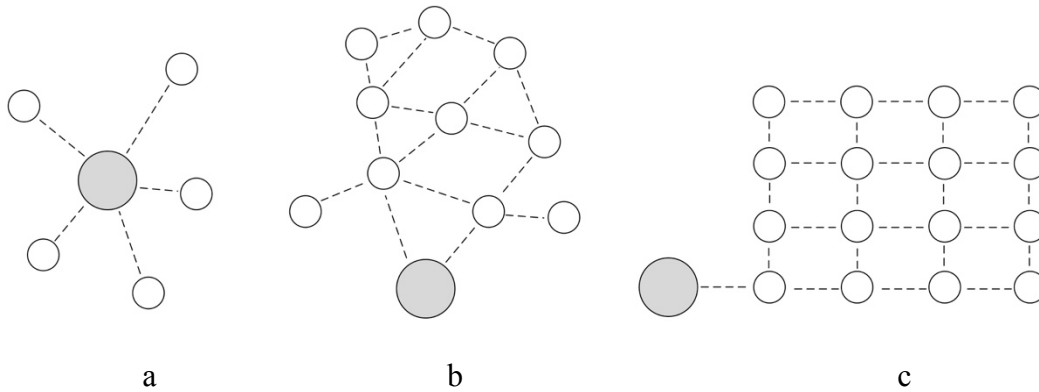


Figura 2.5. Topologías básicas de redes de sensores inalámbricos. (a) red en estrella, (b) red *peer-to-peer*, (c) red tipo malla.

En la Figura 2.5 (a), se presenta una disposición de red básica en estrella compuesta por varios nodos sensores distribuidos alrededor de un nodo de agregación de información central. En esta topología, cada nodo sensor forma un único enlace de comunicación con el nodo de agregación. La Figura 2.5 (b) representa una topología tipo *peer-to-peer* formada varios nodos sensores distribuidos aleatoriamente en un área determinada, y un nodo de agregación de información ubicado en la parte inferior de la red. En esta topología, cada nodo puede establecer múltiples enlaces directos a otros nodos para conformar rutas comunicación redundantes. A su vez, los nodos próximos al nodo de agregación pueden establecer múltiples enlaces directos a otros nodos y al propio nodo de agregación. El tránsito de información desde los nodos receptores, hasta el nodo de agregación se realiza pasando de un nodo a otro, por lo que se producen varios saltos hasta llegar a este, en un proceso denominado *multi-hop*. Esta topología, además de aportar redundancia en la comunicación, permite extender el área de cobertura de los nodos sensores. Por último, la Figura 2.5 (c) muestra una topología de red tipo malla (*grid network*) en la que se observa varios nodos sensores distribuidos uniformemente en forma de cuadrícula para cubrir un área determinada, y un nodo de agregación de información ubicado en la parte inferior de la red. Al igual que en el caso anterior, cada nodo puede

establecer múltiples enlaces directos a otros nodos para completar rutas redundantes, mientras que el nodo más próximo al coordinador es el que envía la información recopilada por toda la red al éste.

La Figura 2.6 representa un ejemplo una topología de red algo más compleja, formada por agrupación de varias topologías básicas. En este caso, cada agrupación de nodos sensores en forma de estrella se denomina *clúster*, y cada nodo de agregación del *clúster* forma, a su vez, enlaces *peer-to-peer* entre ellos. Estos nodos de agregación del cada *clúster*, con capacidad de procesamiento y rangos de transmisión medios, envían la información recopilada a otro nodo de agregación de red centralizado o *Gateway*, con capacidades de procesamiento y radio de transmisión mucho más amplio.

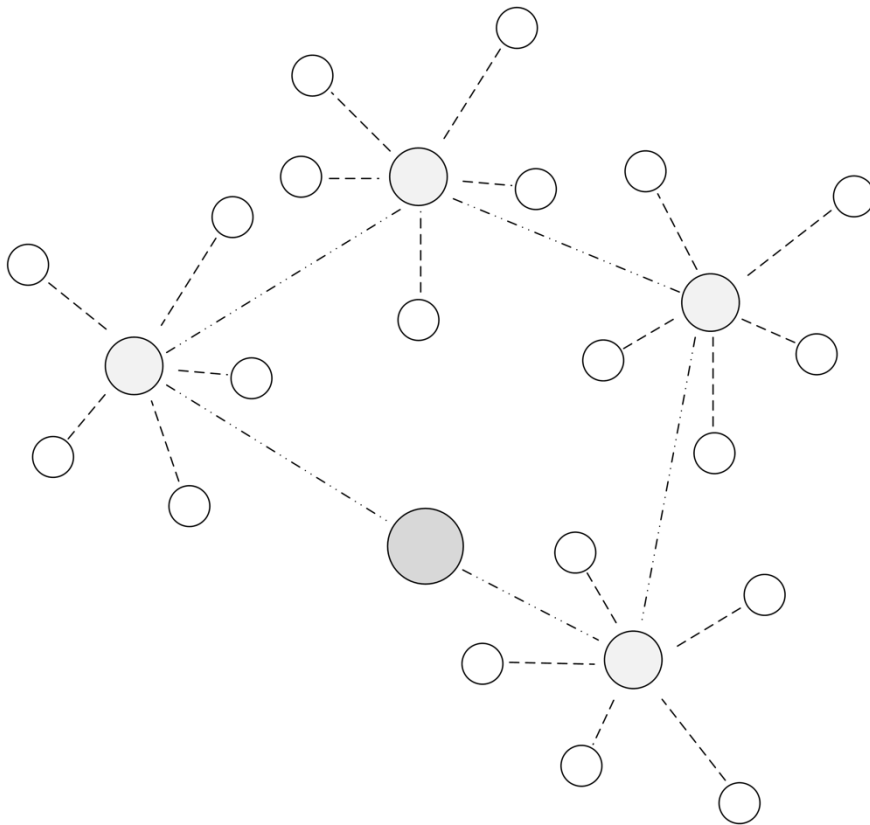


Figura 2.6. Topologías de red con múltiples *clústeres* y nodos de agregación.

Este tipo de redes permiten la transmisión de los datos a mayor distancia, por lo que son adecuadas para aplicaciones que requieran la cobertura de amplias áreas. Por ejemplo, una red de sensores inalámbricos basada en el protocolo *ZigBee* [34] puede desplegarse con hasta 254 nodos, y según la agrupación que se haga, se pueden crear hasta 255 *clústeres* o agrupaciones de nodos con lo cual se puede llegar a tener 64.770 nodos para lo que existe la posibilidad de utilizar varias topologías de red: en estrella, en malla

o en grupos de árboles, permitiéndose en todas ellas un encaminamiento o enrutamiento de saltos múltiples, también conocido como *multi-hop*, facilitando que estas redes puedan abarcar una gran superficie [35]. Si además se incluye un nodo *Gateway* con interfaces duales, por ejemplo, *ZigBee* por el lado de la red de sensores y 5G para el envío de datos hacia la red pública, los rangos de cobertura pueden abarcar grandes distancias.

2.1.4 Aplicaciones de las redes de sensores inalámbricos

El uso de redes de sensores inalámbricos se ha expandido rápidamente en los últimos años, siendo de aplicación una variedad de campos tales como el de la salud, el militar, la vigilancia de infraestructuras críticas o el medioambiente. El objetivo de todas estas aplicaciones es que la información obtenida por los nodos sensores sea accesible en el mundo digital para su procesamiento y análisis, ya sea a nivel corporativo mediante su integración en redes de computadoras, o a nivel más amplio integrándola en arquitecturas como la Web, utilizando tecnologías *Cloud Computing* o el paradigma ya mencionado del *Internet de las cosas*, (*Internet of Things*, IoT). En la mayoría de los casos, estas aplicaciones se centran en la monitorización y recopilación de información del entorno en el que se despliega la red inalámbrica, sin embargo, también existen aplicaciones en las que los nodos sensores realizan algún tipo de actuación o acción de control sobre el entorno.

Con el objetivo de mostrar la diversidad de contextos en los que pueden usarse este tipo de redes, en este apartado se ha tomado una muestra dividiendo las aplicaciones en cinco grupos clasificadas según la naturaleza de su uso: Aplicaciones médico-sanitarias, aplicaciones medioambientales, aplicaciones militares, aplicaciones industriales y aplicaciones urbanas.

2.1.4.1 Aplicaciones médico-sanitarias

Las aplicaciones de las redes de sensores inalámbricos dentro del ámbito de la salud, surgen como respuesta a la necesidad de mejorar los procesos de monitorización en tiempo real y, de recopilación de información sobre el estado de salud de los pacientes, ya sea de forma remota (asistencia domiciliaria) o en los propios centros médicos (hospitales, clínicas, etc.). El uso de las redes de sensores inalámbricos automatiza y

agiliza estas tareas, mejorando la eficiencia y la calidad de la atención a los pacientes. Para ello, se combinan dispositivos portables por el usuario (*wearable hardware*) junto con sensores biomédicos específicos que requieren una precisión muy alta en las mediciones. Estos sensores especiales miden tanto parámetros concretos del estado de salud como las constantes vitales de los pacientes, tales como los medidores de pulso y de frecuencia cardíaca para elaborar electrocardiogramas en tiempo real, medidores de saturación de oxígeno en sangre, y glucómetros, tensiómetros, entre otros. Por otro lado, el uso de las redes de sensores inalámbricos en aplicaciones médicas para conocer el estado de salud de los pacientes de forma remota es ahora uno de los avances más importantes en la vida médica. De este modo, los médicos pueden controlar la presión arterial, la temperatura, la frecuencia cardíaca y otros indicadores de salud del paciente de forma remota, para tomar medidas en caso de cualquier problema de salud. Señalar que, si bien la necesidad de aplicaciones clínicas de las redes de sensores inalámbricos dentro del ámbito de la salud está ampliamente aceptada, ha habido poca experiencia práctica con su implementación en entornos clínicos. Por lo tanto, estas aplicaciones deben considerar desafíos específicos en cuanto a las técnicas y características de diseño a emplear para conseguir implementaciones exitosas en entornos clínicos [36].

2.1.4.2 Aplicaciones medioambientales

Una de las áreas en las que redes de sensores inalámbricos ha tenido gran auge ha sido en el campo de aplicaciones medioambientales. En estos casos se demanda la monitorización continuada de áreas extensas, generalmente de difícil acceso o en entornos hostiles, por lo que el despliegue de estas redes supone una mejora notable en cuanto eficiencia y eficacia. En este sentido, se puede realizar una subdivisión de estas aplicaciones, dependiendo del tipo de datos recopilados y del uso que se hace de éstos entre las que destacan la monitorización de entornos agrícolas (temperatura, humedad del terreno, radiación solar, etc.); seguimiento y vigilancia de entornos naturales (temperatura, cantidad de lluvia, velocidad y dirección del viento, etc.); monitorización de la polución en el aire y en las aguas (contaminantes, SO₂, CO₂, NO_x, partículas en suspensión, etc.); seguimiento y vigilancia de fenómenos naturales destructivos (incendios, terremotos, erupciones volcánicas, inundaciones, etc.); y el seguimiento de

ganado y de animales salvajes (presencia de especies, localización del animal, identificación y detección de movimiento, etc.) [37].

2.1.4.3 Aplicaciones militares

Las aplicaciones militares son consideradas como es el primer campo en el que se comenzó tanto con la investigación como con el desarrollo y uso de las redes de sensores inalámbricos. Dentro de esta categoría, se pueden distinguir, a su vez, varias subcategorías de aplicaciones específicas tales como la monitorización de los combatientes, la vigilancia del campo de batalla o la detección de intrusiones [38]. Para cada una de estas subcategorías o aplicaciones se utilizan nodos equipados con sensores específicos. Como ejemplo, se pueden encontrar sensores específicos de agentes químicos, biológicos, radiológicos, explosivos y tóxicos. También se pueden detectar intrusiones mediante sensores infrarrojos, fotoeléctricos, láser, acústicos y de vibración. De forma similar, se emplean diferentes tipos de sensores para determinar distancias a objetivos de interés o para la obtención de imágenes. En este caso los nodos se equipan con dispositivos tales como el RADAR (*Radio Detection and Ranging*), el LIDAR (*Light Detection and Ranging* o *Laser Imaging Detection and Ranging*), o sensores de infrarrojos entre otros. Además, la flexibilidad que aportan las redes de sensores inalámbricos en cuanto a su arquitectura, les permite adaptarse a diferentes escenarios de guerra, siendo de aplicación tanto en el propio campo de batalla, como en situaciones de guerra urbana [38]. Otras aplicaciones relacionadas con el ámbito militar y que se encuentran en fase de desarrollo de prototipos o en experimentación pueden ser la detección y reconocimiento acústico, el procesamiento de señales acústicas de disparos, sistemas de localización de francotiradores [39].

2.1.4.4 Aplicaciones industriales

La aplicación de la tecnología de las redes de sensores inalámbricos al diseño de redes de área de campo para sistemas de control y comunicación industrial tiene el potencial de proporcionar importantes beneficios en términos de flexibilidad y escalabilidad de instalación en campo, especialmente en aquellas aplicaciones donde existen problemas para el tendido de sistemas cableados. Por ello, el sector industrial es

sin duda otro de los campos más activos tanto en la investigación como en la implementación de las redes de sensores inalámbricos. Dentro de este campo, se pueden encontrar diversas sub categorías de aplicación, entre las que destacan los sistemas de supervisión, control y adquisición de datos SCADA (*Supervisory Control And Data Acquisition*) empleados en industrias tales como la del refino, *Oil&Gas*, producción energética, etc. Estos sistemas requieren la transmisión de datos en tiempo real, y se implementan en aplicaciones como la monitorización de equipos dinámicos (compresores, turbinas, bombas, etc.), supervisión y control de variables de proceso no críticas (temperaturas, presiones, caudales, niveles, densidades de productos, etc.), control de acceso a instalaciones (video, detección de presencia, etc.). En estos casos, los nodos sensores se utilizan para recopilar datos a altas tasas de muestreo, para estudiar los ciclos de trabajo de las máquinas y garantizar su correcto funcionamiento o prever averías; para analizar las variables de proceso y buscar correlaciones entre dichas variables para mejorar el rendimiento de los procesos; o para el envío de datos al laboratorio utilizando comunicación de largo alcance. De este modo, las plantas industriales integran los nodos sensores a los sistemas de control a través de tecnologías mixtas cableadas e inalámbricas para detectar y monitorizar continuamente el estado de los procesos. En este contexto, la tecnología inalámbrica brinda un soporte adecuado a la industria ofreciendo ventajas en términos de bajo coste de instalación, escalabilidad, flexibilidad, falta de cableado, capacidad de procesamiento inteligente, alta movilidad y facilidad de implementación en comparación con las soluciones cableadas convencionales [40]. Dentro de las aplicaciones industriales, las redes de sensores inalámbricos también pueden encontrarse en el sector logístico y del transporte, donde también se requiere la transmisión de datos en tiempo real. Por ejemplo, en el sector de la logística, pueden encontrarse aplicaciones que monitorizan las condiciones de transporte de una determinada mercancía tales como la temperatura y la humedad. Esta monitorización permite aumentar la calidad de la supervisión y disminuir el coste al reducir las pérdidas durante el transporte, especialmente en mercancías que requieren un cumplimiento exhaustivo del mantenimiento de la cadena de frío. En este caso, la monitorización continua de la temperatura de la cadena de suministro mediante sensores y actuadores inalámbricos, pueden permitir realizar acciones de control sobre los parámetros ambientales para mantenerlos en un rango estable, mejorando enormemente el seguimiento y la gestión de estas cadenas [38].

2.1.4.5 Aplicaciones urbanas

Dentro del área de las aplicaciones urbanas de las redes de sensores inalámbricos, la gran variedad de capacidades de detección que éstas ofrecen brinda la oportunidad de obtener un nivel de información sin precedentes sobre un área determinada, ya sea una habitación, un edificio o al aire libre. De hecho, estas redes son una herramienta para medir las características de espaciales y temporales de cualquier fenómeno dentro de un entorno urbano, proporcionando un número ilimitado de aplicaciones. Las aplicaciones de las redes de sensores inalámbricos en el área urbana pueden dividirse en varias sub categorías, siendo las más populares la gestión de hogares inteligentes (*smart homes*), ciudades inteligentes (*smart cities*), sistemas de transporte y monitorización del estado estructuras y edificios [39]. En relación a las aplicaciones de hogares inteligentes, un ejemplo típico es la monitorización de la calidad del aire en el interior de edificios. Para ello se implementan nodos equipados con diversos tipos de sensores que monitorizan parámetros como la temperatura, la humedad relativa o la concentración de dióxido de carbono, para comunicarlos a los usuarios de forma inalámbrica en tiempo real.

2.1.5 Desafíos en el desarrollo e implementación de las redes de sensores inalámbricos

Si bien el uso de redes de sensores inalámbricos se ha expandido rápidamente en los últimos años, la naturaleza de multidifusión de la tecnología inalámbrica, los entornos agresivos en los que se despliegan y las limitaciones en cuanto a capacidad de proceso, memoria y suministro de energía de los propios nodos, son factores que influyen notablemente en el desarrollo e implementación de este tipo de redes. A modo de resumen, algunos de los desafíos que afectan a su diseño recogen aspectos como las limitaciones de recursos y energía, la ubicación y despliegue de los nodos, la recopilación y gestión de datos, la tolerancia a fallos y el mantenimiento, la conectividad inalámbrica y cobertura, la capacidad de auto organización de la red y la ciberseguridad.

2.1.5.1 Limitaciones de recursos y energía de los nodos

Los nodos sensores tienen una capacidad de procesamiento y de almacenamiento de datos muy limitada. Estas limitaciones deben ser consideradas tanto en el diseño de la red como en el del protocolo de comunicaciones a implementar. Estas limitaciones deben considerarse junto con las limitaciones de energía, siendo la conservación de energía un aspecto fundamental en el diseño de la red inalámbrica. Esto se debe a que los nodos sensores son dispositivos autónomos que generalmente obtienen su energía de la batería que incorporan, las cuales tienen una capacidad limitada. Por ello, se hace necesario disponer de un mecanismo de ahorro de energía en cada componente hardware y software del sistema para prolongar la vida útil de cada nodo desplegado y, en consecuencia, la vida útil de la red en su conjunto.

2.1.5.2 Despliegue de los nodos

El despliegue de los nodos es un problema importante y afecta directamente el rendimiento de la red. La gran cantidad de nodos a desplegar y las condiciones del entorno pueden suponer importantes trabas en cuanto a la escalabilidad y confiabilidad de la red inalámbrica. Este despliegue depende de la aplicación y puede afectar en gran medida al rendimiento de la red inalámbrica. Los nodos desplegados deben adaptarse a una aplicación específica y relevante para mantener la conectividad y eficiencia energética en la red. En este contexto, la ubicación de los nodos sensores también es una preocupación en el despliegue. Ésta afecta especialmente al proceso inicial de descubrimiento de rutas, cuando los nodos sensores necesitan obtener información sobre su entorno y sus alrededores para obtener la posición de otros nodos vecinos [41].

2.1.5.3 Agregación y gestión de datos

La agregación de datos define la forma en la que se recopilan los datos en una red de sensores inalámbricos. La agregación de datos y su posterior gestión supone un desafío a tener en cuenta en el despliegue de una red de sensores inalámbricos. Esta agregación puede ser activada por eventos, activada por consultas, activada por tiempo, o híbrida activada por tiempo y evento [41]. En una aplicación típica, los datos son reenviados

mediante retransmisión a través de múltiples saltos usando otros nodos, hasta uno o varios nodos recolectores de información, que pueden usar estos datos localmente o reenviarlos nuevamente otras redes. Esto provoca que, en determinadas circunstancias los nodos sensores puedan generar muchos más datos de los que la propia red puede gestionar, por lo que es importante utilizar métodos de procesamiento de datos que garanticen la calidad y el flujo de datos de manera efectiva. La recopilación de datos activada por un evento que ocurre en o alrededor de la red de sensores, reduce el número de transmisiones al nodo receptor agregando paquetes de datos similares de múltiples nodos fuente y eliminando así la redundancia de datos [41].

2.1.5.4 Gestión del mantenimiento

Dependiendo de la función y el área de implementación de la red de sensores, los nodos pueden permanecer desatendidos durante largos períodos de tiempo, y en ciertas circunstancias algunos nodos pueden fallar o bloquearse debido a la falta de energía, daños físicos o ambientales interferencia. Este hecho requiere una planificación apropiada para llevar a cabo tareas de mantenimiento tales como el reemplazo periódico de baterías del nodo en campo, la inspección periódica del estado de los mismos, etc. Dados los altos costes de mantenimiento asociados, se necesita un modelo de implementación que permita la realización de tareas de supervisión de la propia red de forma remota, quedando las tareas de mantenimiento en campo como último recurso. Por otro lado, el fallo de los nodos no debería afectar la tarea general de la red de sensores ya que, en caso contrario, es posible que se necesiten implementar múltiples niveles de redundancia en la red de sensores, para proporcionar una alta tolerancia fallos [37].

2.1.5.5 Cobertura de la red

La cobertura es un parámetro de diseño muy importante en las redes de sensores inalámbricos. Por una parte, la comunicación inalámbrica dentro de la red puede resultar bastante impredecible debido al uso que se hace en los nodos de transceptores de radiofrecuencia de baja potencia. Además, estas redes se basan en la cooperación entre nodos para crear rutas de comunicación inalámbricas por lo que se espera que haya una densidad de nodos suficiente como para llevar a cabo esta función. Sin embargo, debido

a fallos en los nodos sensores, la topología de la red puede verse afectada con lo que el espacio entre nodos puede aumentar generando problemas de conectividad. Además, cada nodo sensor obtiene datos de su entorno con un determinado radio de cobertura, por lo que las limitaciones en la comunicación inalámbrica pueden provocar no sólo la pérdida de datos, si no también limitaciones en cuanto al alcance y a la precisión de éstos [37].

2.1.5.6 Selección del protocolo de comunicaciones

Un aspecto muy importante en el diseño de una red de sensores inalámbricos, y que está relacionado con los protocolos de comunicaciones que se implementen, es la capacidad de los nodos para organizarse dentro de la red de forma autónoma de tal modo que sean capaces de encontrar las rutas de comunicación de datos más adecuadas. Este tipo de redes suelen desplegarse en modo ad hoc sin que exista una infraestructura previa. Esto requiere que cada nodo sensor sea independiente y lo suficientemente flexible como participar en el encaminamiento mediante el reenvío de datos hacia otros nodos de acuerdo con diferentes situaciones. Si bien esto puede ser visto como un activo, por otro lado, significa que, al no haber una infraestructura fija disponible para la administración de la red, deben contemplarse la implementación de protocolos de comunicación que permitan la formación de nuevos enlaces y rutas desde los nodos hasta el punto de recolección [37]. Por otra parte, en el caso de cambios frecuentes en la estructura de la red, este aspecto debe tenerse en cuenta en el diseño de protocolos de enrutamiento. Es vital mantener estables los datos de enrutamiento en una red donde uno o más componentes de la red son móviles. Este tipo de protocolos se hace indispensable para mantener la tolerancia a fallos de la red en el caso de que se produzca la caída de un número importante de nodos [41].

2.1.5.7 Ciberseguridad

La ciberseguridad debe ser un punto crucial en el diseño e implementación de una red de sensores inalámbricos. Por su propia naturaleza, este tipo de redes tienen características especiales que favorecen nuevas formas de ataques. Si bien en esta misma Tesis se dedicará un capítulo específico sobre este tema, a modo introductorio se exponen en este apartado algunos de los desafíos de Ciberseguridad a los que están expuestas este

tipo de redes. Por ejemplo, los ataques pasivos se llevan a cabo mediante la escucha clandestina de las transmisiones, incluyendo el análisis del tráfico o la divulgación del contenido de los mensajes; mientras que los ataques activos pueden consistir desde la modificación, fabricación e interrupción de los datos, hasta la captura de nodos. Los principales desafíos en materia de ciberseguridad se centran en mantener los principales objetivos dentro de la red, esto es, *confidencialidad* de datos, *disponibilidad* de datos, e *integridad y autenticación* de datos. La *confidencialidad* es un servicio de seguridad básico para mantener el secreto de los datos importantes transmitidos entre los nodos sensores y entre estos y el resto de sistemas que la conforman. La *disponibilidad* de los datos es otra capacidad importante de una red de sensores inalámbricos, pues garantiza el acceso a la información que circula por la red a los nodos o sistemas autorizados cuando sea necesario. La amenaza más perjudicial para la disponibilidad de los datos vendría dada por un ataque de denegación de servicio (*Denial of Service*, DoS) el cual degradaría notablemente la capacidad de comunicación de la red. Por último, la *integridad y autenticación* de los datos son fundamentales garantizar que los datos no han sido manipulados y, verificar si tales datos han sido enviados por un remitente de confianza. Sin autenticación, los atacantes podrían falsificar las identidades de los nodos para difundir información falsa dentro de la red de sensores inalámbricos. Si bien, la confidencialidad, disponibilidad, y la integridad y autenticación de datos son objetivos de ciberseguridad prioritarios, también han de tenerse en cuenta otros servicios de seguridad tales como la *autorización* para asegurarse de que sólo los nodos legítimos puedan acceder a servicios o recursos de la red; y el *no repudio*, para evitar que nodos autorizados y autenticados o los puedan ser rechazados por otros nodos.

Sin embargo, debido a la limitación de los recursos disponibles en los nodos de sensores, arquitecturas de seguridad tradicionales tales como los antivirus, los sistemas de intercambio de claves, o los detectores de intrusiones, no pueden desplegarse con todo su potencial debido a sus requisitos en cuanto a procesamiento, almacenamiento, consumo de energía y sobrecarga de comunicaciones. Esto incrementa considerablemente la probabilidad de ejecutar con éxito diversos ataques contra estas redes. Por otra parte, los nodos sensores pueden ser desplegados a gran escala en áreas abiertas, y en entornos ambientales agresivos, quedando desatendidos. A parte de los posibles problemas causados por el fallo accidental del nodo, la probabilidad de que un sensor desatendido sufra un ataque físico en tal entorno es elevada. Por ejemplo, un atacante podría capturar

el nodo y manipularlo o reprogramarlo con el objetivo de realizar ataques de diversa índole contra la propia red inalámbrica.

Por lo tanto, las redes de sensores inalámbricos han de afrontar retos más complejos desde el punto de vista de la ciberseguridad, introduciendo así más estudios y campos de investigación para hacer frente a estos retos que puedan afectar al normal funcionamiento en términos de disponibilidad, integridad y confidencialidad de los datos.

2.2 Protocolos de comunicaciones en redes

Tal y como se indicó en la definición inicial, una red de sensores inalámbricos se compone de un gran número de pequeños dispositivos denominados nodos que se despliegan de forma extensiva en un determinado entorno para realizar tareas de monitorización, automatización, seguridad, control. Los datos recopilados, son reenviados mediante retransmisión a través de múltiples saltos usando otros nodos, hasta llegar a uno o varios nodos recolectores de información, creando de este modo rutas de comunicación inalámbricas. Este proceso hace que la implementación de los protocolos de transmisión de datos de la red sea más compleja que otro tipo de redes, especialmente desde el punto de vista de las técnicas adoptadas para el enrutamiento de la información entre nodos. Por lo tanto, las necesidades de comunicación, así como la naturaleza de la aplicación de la red, determinarán tanto la arquitectura de la red, como el conjunto de protocolos de comunicaciones a emplear.

2.2.1 Modelos de referencia de arquitectura de protocolos

Para facilitar la adopción de un modelo de protocolo de comunicaciones orientado a las redes de sensores inalámbricos, se emplea un modelo de referencia basado en capas. Para el desarrollo de esta tesis, se utilizará el modelo para Interconexión de Sistemas Abiertos (*Open Systems Interconnection*, OSI) [15]. Partiendo de este modelo conceptual, se pueden desarrollar y comparar diversos protocolos de comunicación estándar tales como la familia de Protocolos de Control de Transmisión y Protocolos de Internet (*Transmission Control Protocol and Internet Protocol*, TCP/IP), o el conjunto de estándares IEEE 802, desarrollados por el Instituto de Ingenieros Eléctricos y Electrónicos (*Institute of Electrical and Electronics Engineers*, IEEE). Dentro de estos

estándares destacan por su uso en redes de sensores inalámbricos los protocolos de la familia IEEE 802.11 (*Wireless Local Area Networks, WLAN*), IEEE 802.15.1 (Bluetooth) o IEEE 802.15.4 (*Wireless Personal Area Networks, WPAN*).

El modelo de referencia OSI (*Open System Interconnection*) describe conceptualmente de forma abstracta mediante una estructura de siete *capas* o *pila*, los procesos de comunicación de un sistema, pero sin tener en cuenta ni la estructura ni la tecnología interna de éste. Esta división en capas de los procesos de comunicación del sistema permite descomponerlo desde el punto de vista lógico en subsistemas independientes más pequeños. El objetivo del modelo es conseguir la interoperabilidad de diversos sistemas de comunicación con protocolos de comunicación estándar [42]. El modelo, que se desarrolló a principios de los años 80, se mantuvo como una referencia y un estándar para la implementación de redes de comunicación hasta los 90, cuando se produjo en despegue y popularización de la Web de Internet. Hoy en día, el modelo de referencia OSI se utiliza como una herramienta de aprendizaje para explicar las funciones de los protocolos de comunicación [43]. La Tabla 2.1 representa de forma esquemática la división en capas del modelo OSI, así como las funciones asignadas a cada una de las capas y la unidad de datos del protocolo (*Protocol Data Unit, PDU*) con la que interactúan.

Capa	Nombre	PDU	Funciones
7	Capa de Aplicación (<i>Application Layer</i>)	Dato (<i>Data</i>)	Proporciona servicios de aplicaciones específicas y procesos de usuario final.
6	Capa de Presentación (<i>Presentation Layer</i>)	Dato (<i>Data</i>)	Esta capa evita problemas de compatibilidad y proporciona formateo, cifrado de datos, etc.
5	Capa de Sesión (<i>Session Layer</i>)	Dato (<i>Data</i>)	Establecimiento, gestión y terminación de conexiones entre aplicaciones.
4	Capa de Transporte (<i>Transport Layer</i>)	Segmento (<i>Segment</i>)	Transferencia completa de datos, responsable de recuperación de errores y control del flujo.
3	Capa de Red (<i>Network Layer</i>)	Paquete (<i>Packet</i>)	Direccionamiento lógico dentro de la red, establecimiento de rutas, control de tráfico, etc.
2	Capa de Enlace de Datos (<i>Data Link Layer</i>)	Trama (<i>Frame</i>)	Direccionamiento físico dentro de la red, control de flujo de datos, sincronización de tramas, etc.
1	Capa Física (<i>Physical Layer</i>)	Bit, Símbolo	Transmisión de bits a través de la red a nivel eléctrico (coaxial, cobre, fibra óptica, Wireless).

Tabla 2.1. Modelo de referencia OSI.

A continuación, se describen de forma más detallada cada una de las funciones asignada a estas capas, así como sus características adicionales.

- 1) La *Capa Física (Physical Layer)* proporciona características mecánicas, eléctricas, funcionales y de procedimiento para establecer, mantener y liberar conexiones físicas (por ejemplo, circuitos de datos) entre entidades de enlace de datos [42]. En esta capa se especifican aspectos de la comunicación tales como el nivel de tensión de trabajo, el modo de sincronización, la velocidad de transmisión de datos, las distancias máximas de transmisión permitida, las bandas de frecuencia en caso de comunicaciones inalámbricas, o el método de acceso al canal entre otros. La función principal asignada a esta capa es, por tanto, la transmisión de bits a nivel electromagnético u óptico, a través del medio que corresponda (coaxial, cobre, fibra óptica, Wireless).
- 2) La *Capa de Enlace de Datos (Data Link Layer)* tiene como propósito proporcionar el medio funcional y de procedimiento para establecer, mantener y liberar enlaces de datos entre entidades de red [42]. Define, por tanto, las características del protocolo encargado de gestionar la conexión entre dos dispositivos conectados físicamente, controlando el flujo de datos entre ellos, además de detectar, y en algunos casos corregir, errores que puedan darse en la capa física. Por ejemplo, el estándar IEEE 802 divide la capa de enlace de datos en dos subcapas la capa de control de acceso al medio (*Medium Access Control, MAC*), y la capa de control de enlace lógico (*Logic Link Control, LLC*). La primera de estas capas es responsable de controlar cómo los dispositivos en una red obtienen acceso al medio y el permiso para transmitir datos; mientras que la segunda se encarga de identificar y encapsular los protocolos de la capa de red, y controlar la verificación de errores y la sincronización de tramas [43]. Las capas MAC y LLC de los estándares IEEE 802, como IEEE 802.3 (Ethernet), IEEE 802.11 (WLAN), IEEE 802.15.1 (Bluetooth) o IEEE 802.15.4 (WPAN), operan en esta capa.
- 3) La *Capa de Red (Network Layer)* proporciona un modo funcional y los medios de procedimiento para intercambiar unidades de datos de servicio de red entre dos entidades de transporte a través de una conexión de red. Proporciona a las entidades de transporte con independencia del enrutamiento [42]. En otras palabras, la capa de red entrega datos en forma de paquetes desde el origen hasta el destino, creando rutas a través de tantos enlaces como sea necesario. La mayor diferencia entre la capa de red y la capa de enlace de datos es que la

capa de enlace de datos está a cargo de la entrega de datos entre sistemas adyacentes (sistemas conectados directamente a un salto de distancia), mientras que la capa de red entrega datos a sistemas que no están conectados directamente a la fuente. Puede haber muchos tipos diferentes de enlaces de datos y capas físicas en la red, dependiendo de la variedad de tipos de enlaces, pero la capa de red es esencialmente la misma en todos los sistemas [43]. El concepto clave en esta capa es la dirección de red, ya que es ésta la que proporciona información al receptor sobre de donde vino el paquete, y por lo tanto hacia dónde tiene que enviar su respuesta. En la familia de protocolos TCP/IP, la función de la capa de red la realiza el protocolo de internet IP (*Internet Protocol*), el cual interpreta y gestiona las direcciones IP para distribuir los paquetes de datos por la red.

- 4) La *Capa de Transporte (Transport Layer)* se implementa para proporcionar un servicio de transporte universal en asociación con los servicios subyacentes proporcionados por las capas inferiores. Esta capa proporciona una transferencia de datos transparente entre entidades de sesión, liberando a las entidades de sesión de cualquier preocupación sobre los detalles y el modo en la que se logra una transferencia de datos confiable y rentable. La capa de transporte es necesaria para optimizar el uso de servicios de comunicaciones disponibles para proporcionar el rendimiento requerido para cada conexión entre entidades de sesión a un costo mínimo [42]. Si la capa de red reenvía todos los paquetes de forma independiente sin reconocer ninguna relación entre éstos, la capa de transporte, por el contrario, puede asegurarse de que todo el mensaje, a menudo distribuido en una secuencia de paquetes, llegue en orden y sin errores. Este proceso de dividir el contenido del mensaje en paquetes se conoce como segmentación. Esta función de la capa de transporte implica la implementación de mecanismos de control de flujo y de errores [43]. En la familia de protocolos TCP/IP, el protocolo de control de transmisión TCP (*Transmission Control Protocol*) es el que realiza todas estas funciones.
- 5) La *Capa de Sesión (Session Layer)* tiene el propósito de ayudar en las interacciones entre entidades de presentación colaboradoras. Para hacer esto, la capa de sesión proporciona servicios que se clasifican en las siguientes

categorías: (a) Vincular dos entidades de presentación en una relación, y desvincularlas. Esto se denomina *servicio de administración de sesiones*. (b) Control del intercambio de datos, y operaciones de delimitación y sincronización de datos entre dos entidades de presentación. Esto se denomina *servicio de diálogo de sesión*. Para implementar la transferencia de datos entre entidades de presentación, la capa de sesión puede emplear los servicios prestados por la capa de transporte [42]. Protocolos como L2TP (*Layer 2 Tunneling Protocol*), NetBIOS (*Network Basic Input Output System*), RPC (*Remote Procedure Call Protocol*), o RTCP (*Real-time Transport Control Protocol*), entre otros, se encuentran en esta capa.

- 6) La *Capa de Presentación (Presentation Layer)* tiene como propósito principal proporcionar el conjunto de servicios que puede seleccionar la capa de aplicación para permitirle interpretar el significado de los datos intercambiados. Estos servicios son para la gestión del intercambio de entrada, visualización y control de datos estructurados [42]. El servicio de presentación es independiente de la ubicación y se considera que está por encima de la capa de sesión, que proporciona el servicio de vincular un par de entidades de presentación. Mediante el uso de los servicios proporcionados por la capa de presentación, las aplicaciones en un entorno de interconexión de sistemas abiertos pueden comunicarse sin costos inaceptables en la variabilidad de la interfaz, las transformaciones o la modificación de la aplicación [42].
- 7) La *Capa de Aplicación (Application Layer)* representa la capa más alta de la arquitectura OSI. Los protocolos de esta capa sirven directamente al usuario final, proporcionando el servicio de información distribuida apropiado para una aplicación, para su gestión y para la administración del sistema [42]. La gestión de la interconexión de sistemas abiertos comprende las funciones necesarias para iniciar, mantener, rescindir y registrar los datos relativos al establecimiento de conexiones para la transferencia de datos entre procesos de aplicación. Las otras capas existen solo para soportar esta capa. Una aplicación se compone de procesos de aplicación cooperantes que se intercomunican de acuerdo con los protocolos de la capa de aplicación [42]. Los procesos de aplicación son la fuente y el sumidero definitivos para el intercambio de datos. Una parte de un proceso de aplicación se manifiesta en la capa de aplicación

como la ejecución del protocolo de aplicación, es decir, entidad de aplicación [42]. Protocolos como Telnet, FTP (*File Transfer Protocol*), SMTP (*Simple Mail Transfer Protocol*), SSH (*Secure Shell*), TLS (*Transport Layer Security*), entre otros, desempeñan sus funciones en la capa de aplicación.

2.2.2 Protocolos de comunicación para redes de sensores inalámbricos

Tomando como referencia la Tabla 2.1, dependiendo de la solución adoptada para el protocolo de comunicación en la red de sensores inalámbricos que se adopte, así como del dispositivo que lo implemente, se utilizarán diferentes capas funcionales del modelo OSI. A modo de ejemplo, un nodo sensor básico debe contar al menos con las capas 1, 2 de la pila de protocolos, mientras que un nodo de agregación o que realice funciones de enrutador deberá incluir además de las capas anteriores, al menos la capa 3. Si además el dispositivo realiza funciones de formato de datos o ejecuta aplicaciones específicas, deberá incluir al menos la capa 7.

A modo de ejemplo, *ZigBee* [35] es uno de los estándares más empleados tanto en redes de sensores inalámbricos como en redes IoT inalámbricas. Esta especificación, que se encuentra en constante evolución, define una arquitectura de pila de protocolo basada en 4 capas. Las dos primeras capas, corresponden a los niveles 1 y 2 según el modelo OSI, esto es, la capa física y la capa de control de acceso al medio. Estas capas se sustentan en el estándar IEEE 802.15.4 [44]. Por otro lado, la especificación define dos capas superiores, la capa de red y la capa de aplicación, que corresponden con los niveles 3 y 7 del modelo OSI, ofreciendo por tanto una pila de protocolos completa para crear redes inalámbricas de área privada de baja velocidad, o *Low-Rate Wireless Private Area Networks* (LR-WPANs). En estas capas superiores tienen cabida una gran variedad de protocolos de enrutamiento e interfaces de aplicación, lo que le permiten a la especificación una gran versatilidad de uso. Por ejemplo, en la capa de aplicación, se definen los objetos de dispositivo *ZigBee* (ZDO, *ZigBee Device Objects*) que son responsables de incluir y realizar un seguimiento de los roles de los nodos de la red, administrar las solicitudes de éstos para unirse a una red, así como el descubrimiento y la seguridad de los nodos. Además, la capa de aplicación incluye aplicaciones definidas por el fabricante [45]. En cuanto a la capa de red, ésta define aspectos como el enrutamiento, permitiendo adoptar cualquiera de las múltiples topologías vistas anteriormente, y la

seguridad de las comunicaciones, implementado el cifrado y la autenticación de datos. En esta capa se pueden implementar protocolos de enrutamiento como AODV (*Ad-hoc On-demand Distance Vector*) o DSR (*Dynamic Source Routing*), o estándares de seguridad como el cifrado avanzado AES (*Advanced Encryption Standard*) entre otros.

Si bien en la literatura de referencia puede encontrarse un amplio abanico de estándares y protocolos utilizados en redes de sensores inalámbricos, con el fin de no extender este capítulo, en las siguientes secciones se describen con más detalle los protocolos que se utilizarán como base para llevar a cabo los experimentos para la validación de los modelos epidemiológicos propuestos en esta Tesis. En cualquier caso, cabe destacar la importancia en el mundo de las redes de sensores inalámbricos de protocolos como *Wireless HART* (estándar IEC 62591) [46], *ISA-100.11a* [47], *IETF IPv6-6LoWPAN* [48], o *LoRaWAN* [49], por mencionar algunos de los más relevantes.

2.2.2.1 Fundamentos del protocolo IEEE 802.15.4

Como se indicó anteriormente, el estándar IEEE 802.15.4 es sin duda uno de los más ampliamente utilizados en la actualidad, para conformar la primera parte de la pila de protocolos de comunicación según el modelo OSI (*Open System Interconnection*). De hecho, además de *ZigBee*, otros estándares como los mencionados *6LoWPAN*, *Wireless HART*, o *ISA 100.11a*, hacen uso de IEEE 802.15.4, cuya última revisión data de julio de 2020 [44]. El objetivo de esta tecnología no es proporcionar velocidades muy altas de comunicación, de hecho, la tasa de transmisión máxima está en 250 kbps, si no poder construir nodos inalámbricos cuyos transceptores de radio frecuencia tengan un reducido consumo energético. El estándar IEEE 802.15.4 define la capa Control de Acceso al Medio (MAC, *Medium Access Control*) y la capa física (PHY, *Physical Layer*). Además, y con objeto de reducir el consumo de energía de los nodos sensores disminuyendo el ciclo de trabajo mientras permanecen inactivos, el estándar define dos tipos de dispositivos de red, denominados dispositivos de función reducida o RFD (*Reduced Function Device*), y dispositivos de función completa o FFD (*Full Function Device*). El primer tipo de nodos, no puede ejercer como coordinador de red y, por ejemplo, en una arquitectura en estrella, sólo podría actuar como uno de los vértices de esta. Sin embargo, los dispositivos tipo FFD puede convertirse en nodos coordinadores. Por ejemplo, en topologías tipo estrella un dispositivo FFD que inicia la comunicación se convierte en el

coordinador de red. Mientras que, en una topología tipo malla, los dispositivos FFD pueden comunicarse entre ellos y además pueden encaminar tráfico entre otros nodos de la red. Cabe señalar que, en topologías con configuración en estrella como la indicada en la Figura 2.5 (a), una red de sensores inalámbricos requiere al menos un dispositivo FFD que actúe como coordinador de la red y los demás dispositivos pueden ser del tipo RFD para reducir el coste del sistema. Para topologías *peer-to-peer* o malladas como las indicadas en la Figura 2.5 (b) y (c), así como en topologías con múltiples *clústeres* como la presentada en la Figura 2.6, todos los dispositivos deben ser FFD [45].

Con respecto a la capa física, sus funciones principales son la selección de frecuencia, la generación de la frecuencia portadora, la detección de la señal y la modulación de ésta. El estándar ofrece dos bandas base como frecuencia de operación la banda de 850 a 930 MHz, y la banda de 2450 MHz, ambas empleando técnicas de espectro expandido de secuencia directa DSSS (*Direct Sequence Spread Spectrum*), para modular posteriormente la señal en una portadora para su transmisión. La primera de las bandas permite velocidades de transferencia de entre 20 y 40 kbps, mientras que la segunda ofrece velocidades de 250 kbps, con coberturas de hasta 80 metros de radio para potencia de transmisión de 1mW. Por otra parte, la modulación DSSS incorpora una redundancia en cada bit de datos, distribuyéndolos por el ancho de banda utilizado. Esta redundancia permite no sólo identificar los datos como pertenecientes a un determinado nodo, sino por supuesto, facilita la detección de errores. Al distribuir los datos en todas las frecuencias de la banda, la señal resultante se parece cada vez más al ruido, lo que la hace más resistente a las interferencias [45]. Además, la capa física puede determinar si los canales están ocupados utilizando un método CCA (*Clear Channel Assessment*). Este método permite reportar canales libres según el sentido de la portadora de las señales DSSS, y/o si el parámetro detección de energía denominado ED (*Energy Detection*) está por encima del límite del canal [45].

En cuanto a la capa Control de Acceso al Medio (MAC), ésta se encarga de controlar el acceso al canal de radio usando el mecanismo de detección de portadora y prevención de colisiones CSMA/CA (*Carrier Sense Multiple Access with Collision Avoidance*). El estándar admite en esta capa dos modos de operación denominados *beacon-enabled* y *non-beacon-enabled*. En el modo *beacon-enabled* los nodos que actúan de enrutadores, transmiten periódicamente una especie de baliza como señal para confirmar su presencia en la red. Para este modo de operación se emplea una estructura

de datos denominada *supertrama*. Esta estructura tiene como objetivo proveer ancho de banda libre y proporcionar baja latencia en las transmisiones. La *supertrama* está delimitada por las tramas de tipo baliza, y tiene un periodo de tiempo asignado durante el cual deben realizarse todas las transmisiones, periodo que puede estar entre 15 ms y 252 s. A su vez, el tiempo total de cada *supertrama* se divide equitativamente en 16 intervalos de tiempo o *slots*. De este modo se garantiza que el acceso al canal radio dentro de cada *slot* estará libre de colisiones [45].

La Figura 2.7 presenta la estructura típica de una *supertrama* IEEE 802.15.4 para el modo de baliza habilitada, donde SD (*Superframe Duration*) representa la duración del periodo o porción activa de la *supertrama*. A su vez, dentro de esta porción activa, se distinguen dos periodos, consta de dos periodos, denominados periodo de contención de acceso (CAP, *Contention Access Period*) y el periodo libre de contención (CFP, *Contention Free Period*). Durante el periodo CAP, los nodos utilizan el algoritmo CSMA/CA para acceder al canal, mientras que durante el periodo CFP, se pueden asignar hasta 7 ranuras de tiempo o sub-periodos denominados servicios de transmisión garantizada (GTS, *Guaranteed Transmission Services*), lo que permite que el nodo opere en el canal que está dedicado exclusivamente a ello [50]. Esto logra un compromiso razonable entre consumo de energía y retardo de la transmisión, por lo que los GTS permiten servicios de datos en tiempo real.

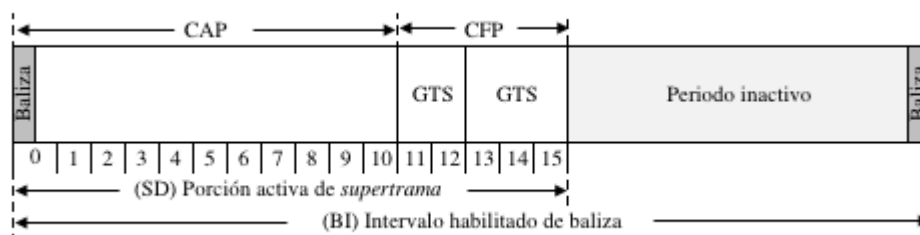


Figura 2.7. Estructura típica de una *supertrama* IEEE 802.15.4.

Dentro del modo *beacon-enabled*, el estándar IEEE 802.15.4, define, a su vez, dos mecanismos de sincronización denominados seguimiento de baliza y seguimiento sin baliza. En el primero de los mecanismos, el nodo intenta adquirir la baliza y seguirla, rastreándola de forma regular mediante la activación oportuna de su receptor radio. Después de la transmisión, si el nodo ya no tiene más datos para enviar, éste pasa a modo hibernación o *sleep*, pero mantendrá activo el rastreo de la baliza. Por el contrario, si no

se especifica el seguimiento, el nodo intenta adquirir la baliza solo cuando necesite enviar datos, dejando de seguirla una vez finalizado el envío de dichos datos [50].

Por otra parte, el modo *non-beacon-enabled*, los nodos se mantienen continuamente activos, esto es, no se dispone de una baliza que indique el intervalo de tiempo asignado durante el cual deben realizarse todas las transmisiones. Si bien este modo puede reducir notablemente la latencia en las comunicaciones, dependiendo de la aplicación, también puede resultar más difícil sincronizar los intervalos de tiempo para la transmisión, lo que obliga a mantener todos los nodos activos. Este modo conlleva, por tanto, un mayor consumo de energía por parte de los nodos, aunque puede ser empleado de manera eficiente en redes tipo estrella como la presentada en la Figura 2.5 (a), implementando en los vértices nodos del tipo RFD (*Reduced Function Device*), mientras que como nodo central se implementa un dispositivo del tipo FFD (*Full Function Device*).

Por último, cabe mencionar en este apartado algunas consideraciones adicionales sobre Ciberseguridad relacionadas con el protocolo IEEE 802.15.4. Si bien como ya se ha mencionado, el estándar es uno de los más ampliamente utilizados en aplicaciones de comunicaciones inalámbricas de corto alcance, donde se requieren bajas tasas de transferencia, como por ejemplo en las redes inalámbricas IoT, los riesgos derivados de una posible falta de seguridad en cuanto a disponibilidad, integridad y confidencialidad de los datos pueden disuadir de su utilización en ciertos entornos. Para abordar este problema el estándar introduce varias soluciones de seguridad, definidas en diferentes *Amendments*, como por ejemplo el IEEE 802.15.4y (*Amendment 3*). Esta enmienda define extensiones de seguridad para el estándar agregando AES-256-CCM, junto con un registro de método de autenticación y conjunto de cifrado, y un proceso para la inclusión de algoritmos adicionales. El registro define una capacidad para alinear el IEEE 802.15.4 con los requisitos de seguridad de los estándares de capas superiores [51]. Estas extensiones de seguridad que, definen la posibilidad de proteger paquetes a nivel de la capa MAC mediante técnicas de criptografía de clave simétrica avanzada con varias opciones de seguridad, basadas en un algoritmo de contador con código de autenticación de mensajes de encadenamiento de bloques de cifrado AES-CCM* (CCB-MAC, *Counter with Cipher Block Chaining Message Authentication Code*). Entre las opciones mencionadas se definen 8 niveles de seguridad; un campo específico dentro del encabezado MAC con los parámetros que permiten al nodo destino descifrar el mensaje recibido; un mecanismo para identificar de forma única una determinada clave de entre

todas las disponibles, basado en el conocimiento de la dirección MAC del nodo que generó el paquete; y procedimientos dedicados para gestionar el cifrado y el descifrado de las tramas MAC [51].

Estas extensiones suponen un avance importante en cuanto a mejora de la Ciberseguridad del estándar, sin embargo, éste aún no explica cómo gestionar la inicialización de un dominio IEEE 802.15.4 seguro, la generación e intercambio de claves, y la gestión de operaciones de adhesión de nodos en una red segura ya configurada. Estas operaciones son soportadas habitualmente por capas de protocolos superiores donde se adaptan al dominio de las redes de sensores inalámbricos, y también al dominio de las redes IoT inalámbricas, mecanismos de seguridad conocidos y de uso habitual en redes convencionales.

2.2.2.2 Fundamentos de protocolos de enrutamiento

Como se ha indicado en el apartado anterior, el estándar IEEE 802.15.4 conforma la primera parte de la pila de protocolos de comunicación según el modelo OSI, si bien para disponer de una pila completa, es preciso definir varias capas superiores, que al menos como se vio en el caso del protocolo deben incluir, una capa de red y una capa de aplicación. En este sentido, protocolos como los ya mencionados *Wireless HART* [46], *ISA-100.11a* [47], *IETF IPv6-6LoWPAN* [48], o *LoRaWAN* [49], por mencionar algunos de los más relevantes dentro del mundo de las redes de sensores inalámbricos, ofrecen la pila de protocolo completa para la construcción de los nodos.

Dentro de la pila de protocolos, la capa de red juega también un papel fundamental, dando cabida, entre otros, a los protocolos encargados de enrutamiento. La función principal de un protocolo de enrutamiento es determinar rutas para que los nodos sensores transmitan datos en una red mientras se logra maximizar la vida útil de la red, la cual depende principalmente de la vida útil de los nodos sensores en la red [41]. En este sentido, las capacidades de resiliencia de una red de sensores inalámbricas pueden proporcionarse mediante mecanismos de autoconfiguración y adaptación implementados en los protocolos de enrutamiento, los cuales pueden cambiar la topología según el estado y disponibilidad de los caminos, el consumo energético, el balance de tráfico, o la calidad de servicio, entre otros.

Los protocolos de enrutamiento se pueden clasificar en función de diferentes criterios, como por ejemplo según el modo en el que el protocolo establece la ruta entre los nodos y entre éstos y el nodo de agregación de datos [52], o según los diferentes tipos o características de los nodos sensores que conforman la red [41]. Tomando como referencia la primera clasificación, los protocolos se dividen en tres grupos con diferentes categorías, tal y como puede verse en la Figura 2.8.

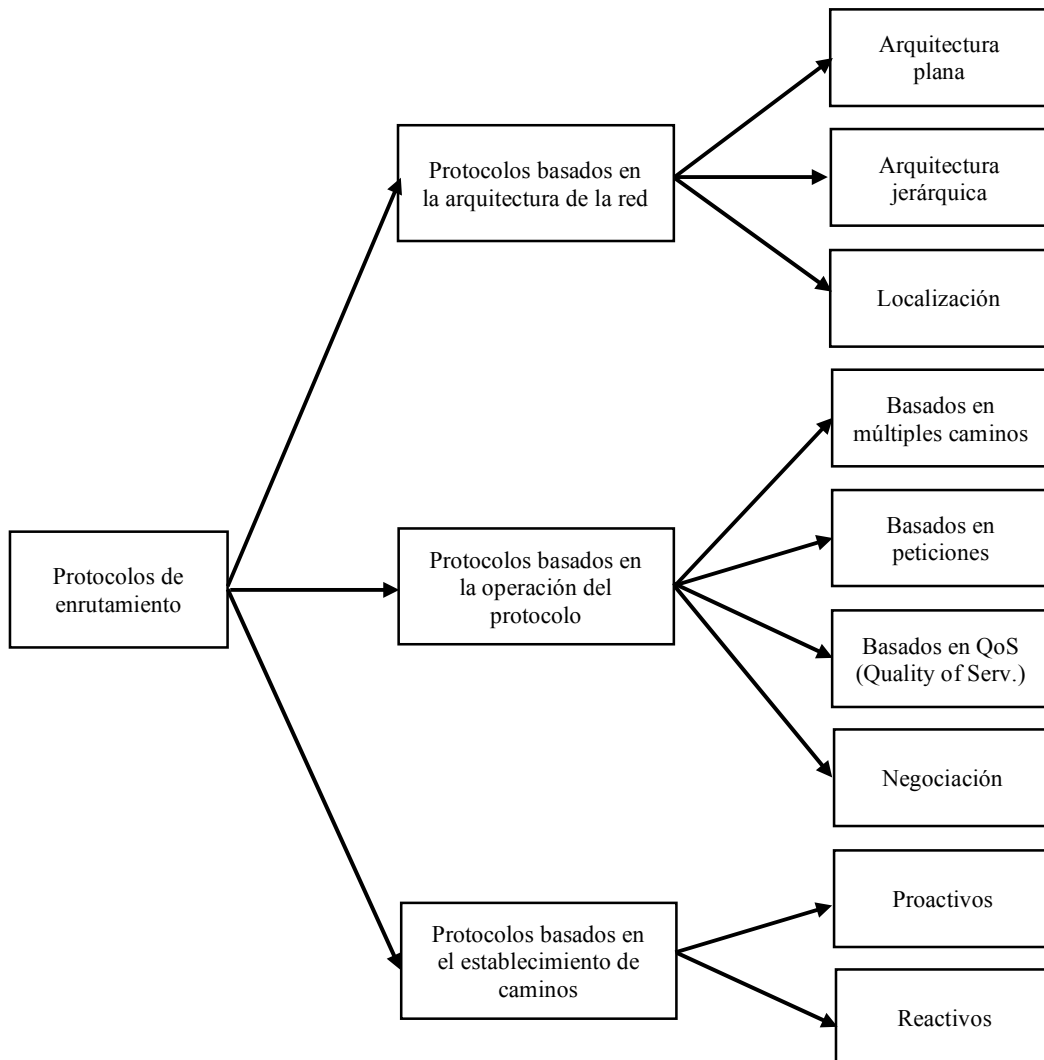


Figura 2.8. Clasificación de los protocolos de enrutamiento según el modo en el que establecen la ruta entre los nodos.

Por señalar algunos ejemplos, dentro de los protocolos de enrutamiento basados en la arquitectura de red, en los de estructura jerárquica, los nodos que conforman la red tienen distintas capacidades y, por tanto, los nodos de mayor capacidad realizan tareas críticas mientras que las tareas menos críticas se asignan a nodos con baja capacidad.

Además, la red puede estructurarse en dos o más niveles jerárquicos [52]. Protocolos basados en clústeres como LEACH (*Low-Energy Adaptive Clustering Hierarchy*) entran en este grupo de protocolos jerárquicos. Aquí los nodos con mayores capacidades actúan como *cabeceras de clúster* (CH, *Cluster Head*), recopilando la información de todos los nodos del clúster, agregando y comprimiendo posteriormente los datos para enviarlos al nodo recolector principal de la red, nodo sumidero o *sink node*.

Por otra parte, o según los diferentes tipos o características de los nodos sensores que conforman la red se puede generar una clasificación tanto de las propias redes como de los protocolos utilizados en homogéneas y heterogéneas. Las redes de sensores inalámbricas homogéneas se componen de nodos que son similares o son del mismo tipo. La similitud puede ser con respecto al ancho de banda de comunicación, su fuente de energía, capacidad de procesamiento, o la capacidad de almacenamiento. Por ejemplo, en el caso de una red homogénea, la selección de los nodos de *cabecera del clúster* (CH, *Cluster Head*) se asigna aleatoriamente. Por otro lado, las redes de sensores inalámbricos heterogéneas, están formadas por nodos con diferentes capacidades de procesamiento y diferentes tipos de sensores, incluso diferentes protocolos de comunicación [41].

Si bien basándose en ambas clasificaciones se podrían enumerar una gran cantidad de protocolos, con el fin de no extender este Capítulo, en este apartado se presentan a modo introductorio, las características fundamentales de los protocolos de enrutamiento empleados como base para los experimentos llevados a cabo en esta Tesis. Los tres protocolos de enrutamiento enumerados desempeñan principalmente funciones de autoconfiguración de la red. Por una parte, *Ad-hoc On-demand Distance Vector* (AODV) y *Dynamic Source Routing* (DSR) son protocolos de enrutamiento basados en el establecimiento de caminos y de tipo reactivo, ya que, en ambos casos, los nodos actualizan las rutas cuando se requieren. Por otra parte, también cabe mencionar al protocolo *Multi-Parent Hierarchical Protocol* (MPH), en el que los nodos actualizan las rutas periódicamente o bien cuando se detectan cambios en su entorno.

El protocolo de comunicaciones *Ad-hoc On-demand Distance Vector* (AODV) [53] permite que los nodos de una red puedan responder a los cambios frecuentes en la topología de la y las interrupciones en la conectividad del enlace. Esto es posible gracias a los números de secuencia de destino que siempre garantizan bucles libres en la red. A grandes rasgos, el funcionamiento para la conformación de rutas puede describirse como sigue. En primer lugar, un nodo en modo de transmisión envía un paquete de solicitud de

ruta RREQ (*Route Request*). Un nodo vecino que recibe este paquete, primero verifica en su registro si ya han recibido previamente este mismo paquete RREQ. Si éste no está registrado, el nodo lo retransmite nuevamente, incrementando el número de saltos y trazando una ruta inversa, desde el nodo final al que ha llegado este RREQ. El nodo que recibe el paquete RREQ solo puede responder para confirmar una ruta con un paquete de respuesta de ruta RREP (*Route Response*) en los siguientes casos: si el nodo ya es el destino o si el nodo tiene una ruta disponible al destino. En AODV, los paquetes RREP no se generan mediante nodos de reenvío incluso si tienen rutas válidas y, por lo tanto, evitan agregar sobrecargas de respuestas múltiples [41]. Este procedimiento se repite de forma continua hasta que se alcanza el nodo origen que solicitó la ruta. Este nodo de origen puede recibir paquetes RREP de diferentes nodos como confirmación de la existencia de múltiples rutas posibles para alcanzar al nodo destino. En este caso, el nodo elegirá generalmente la ruta que tiene el menor número de saltos, aunque opcionalmente, puede optar por seleccionar como ruta más adecuada aquella que tiene el número de secuencia más alto [22].

En el caso del protocolo y *Dynamic Source Routing* (DSR) [54], el establecimiento de rutas sigue el siguiente proceso. Cuando un nodo tiene un paquete para enviar a un determinado destino, primero comprueba en su registro si ya dispone de una ruta establecida hasta el nodo destino; si es así, genera un nuevo encabezado en el paquete a enviar con la ruta y los salta para llegar al destino, y lo envía. Si no dispone en su registro de una ruta a ese destino, el nodo inicia el mecanismo de descubrimiento de ruta, donde el nodo origen envía un paquete de difusión RREQ (*Route Request*) con la ruta solicitada, que contiene el identificador del nodo de origen y del nodo destino; este paquete contiene también un identificador único para el RREQ. Cada nodo intermedio hace una copia del paquete RREQ recibido y agrega su identificador. Cuando un nodo recibe un RREQ, primero busca en su registro para comprobar si tiene la ruta al nodo de destino. Si es así, antes de reenviar el RREQ, el nodo en cuestión responde con un RREP (*Route Response*) al nodo origen. En este paquete RREP, el nodo incluye todos los nodos por los que ha pasado el paquete RREQ recibido, y los nodos de la ruta que se encuentran en su registro. Si el nodo no encuentra una ruta en su registro, éste agrega su dirección al paquete RREP y lo reenvía por difusión (*broadcast*). Una vez que el nodo origen recibe el paquete RREP, almacena la ruta en su registro. Esta ruta se incluirá en el encabezado de cada paquete posterior que este nodo envíe, de tal modo que todos los nodos que reciban el paquete

sepan a qué nodo siguiente deben reenviarlo. Al igual que con AODV, los nodos pueden tener varias rutas a un mismo nodo destino y, por lo tanto, pueden elegir aquella que contemple el número de saltos más bajo [22].

Finalmente, el protocolo *Multi-Parent Hierarchical Protocol* (MPH) [55] es un protocolo de enrutamiento que crea una topología de red lógica de tipo jerárquico, donde la jerarquía de nodos se determina de tal modo que cuanto más bajo es el nivel, más baja es la jerarquía. De este modo, la jerarquía más alta o la jerarquía raíz está representada por el nodo coordinador. Cuando un nodo está en un nivel jerárquico específico, los nodos que están conectados a él y tienen un nivel jerárquico superior son nodos padres. Por otro lado, los nodos que están conectados a cualquier nodo padre y que tienen un nivel jerárquico más bajo son nodos hijos. La topología jerárquica se formará con rutas que minimicen el número de saltos desde un nodo dado hasta el coordinador, esta restricción reducirá el consumo total de energía de la red inalámbrica [55].

El protocolo MPH utiliza principalmente tres tipos de paquetes: los paquetes de descubrimiento de red ND (*Network Discovery*), respuesta de descubrimiento de vecinos NDR (*Neighbour Discovery Response*) y respuesta de reconocimiento de descubrimiento de vecinos NDRACK (*Neighbour Discovery Response Acknowledge*). En el estado inicial, si el nodo es el coordinador entonces se establece su jerarquía al valor máximo, de lo contrario, simplemente se pone a cero. Posteriormente, cada nodo envía periódicamente paquetes ND para iniciar el descubrimiento y actualización de sus vecinos. Cuando un nodo recibe un paquete ND, responde con un paquete NDR, que incluye su información jerárquica. El nodo que recibe un paquete NDR responderá con un paquete NDRACK que también incluye su nivel jerárquico. Cuando un nodo tiene datos para transmitir, crea un paquete MPH y lo envía a un nodo padre; si el nodo padre que recibe el paquete es el coordinador, entonces el paquete ha llegado a su destino; de lo contrario, el paquete se reenviará a cualquiera de los nodos principales [55].

Dentro de una red de sensores inalámbricos, sus capacidades de resiliencia pueden proporcionarse mediante mecanismos de autoconfiguración y adaptación implementados las diferentes capas del protocolo de comunicación. Dado que en todos los escenarios propuestos en los experimentos se utilizan los mismos protocolos en la capa física y en la capa MAC, la resistencia a ataques de la red de sensores inalámbricos a estudio puede considerarse intrínsecamente relacionada con los protocolos de enrutamiento utilizados. A pesar de las diferencias mencionadas anteriormente, los tres protocolos de enrutamiento

utilizan mecanismos de autoconfiguración para conformar y actualizar la topología de la red, cuando cambian las condiciones del entorno inalámbrico.

2.3 Conclusiones

En este capítulo introductorio sobre fundamentos de redes de sensores inalámbricos, se ha revisado el estado actual del arte en cuanto a la tecnología de redes de sensores inalámbricos, proporcionando una visión general que incluye desde aspectos como los elementos hardware y software que componen estas redes, hasta las arquitecturas y protocolos sobre los que se sustenta, además de las aplicaciones actuales, los retos en su despliegue y sus perspectivas de evolución en el ámbito del Internet de las cosas (*Internet of Things*, IoT).

Además, se han mencionado las aplicaciones en las que actualmente se pueden encontrar este tipo de redes clasificándolas según la naturaleza de su uso, esto es, aplicaciones médico-sanitarias, aplicaciones medioambientales, aplicaciones militares, aplicaciones industriales y aplicaciones urbanas. También se ha prestado atención, a algunos de los desafíos que afectan a su diseño mencionando aspectos tales como las limitaciones de recursos y energía, la ubicación y despliegue de los nodos, la recopilación y gestión de datos, la tolerancia a fallos y el mantenimiento, la conectividad inalámbrica y cobertura, la capacidad de auto organización de la red y la ciberseguridad.

Por último, se ha hecho una descripción del estándar IEEE 802.15.4 ya que, sin duda, unido a otros protocolos en las capas superiores del modelo OSI, es uno de los más ampliamente utilizados en la actualidad para la configuración de este tipo de redes.

CAPÍTULO

3

Fundamentos de Ciberseguridad en redes de sensores inalámbricos

Las redes de sensores inalámbricos se despliegan de forma extensiva en un determinado entorno para realizar tareas de monitorización, automatización, seguridad, control y en general cualquier otra aplicación que requiera la recopilación de datos en tiempo real. Sin embargo, debido al despliegue de estas redes en entornos agresivos o desatendidos –sin que incorporen hardware resistente a la manipulación– a la naturaleza inalámbrica del canal de comunicación, y a las limitaciones en los recursos de los nodos, tales como su capacidad de procesamiento, fuente de alimentación, etc., hace que este tipo de redes sean vulnerables a determinadas amenazas y ataques.

En este Capítulo se abordan los aspectos principales relacionados con la Ciberseguridad en redes de sensores inalámbricos, aportando una visión de conjunto sobre las principales amenazas y ataques, así como de los mecanismos y sistemas de seguridad que habitualmente se implementan en este tipo de redes.

3.1 Introducción

En los últimos años, la adopción de tecnologías de redes de sensores inalámbricos ha aumentado considerablemente, surgiendo nuevos paradigmas como la Industria 4.0 o el Internet de las Cosas (*Internet of Things*, IoT) entre otros. Si bien los dispositivos utilizados en el despliegue de las redes de sensores inalámbricos suelen estar limitados en cuanto a capacidades de computación o memoria, este hecho no puede considerarse como una barrera natural frente a ciertos tipos de ataques. Aunque existen ataques específicos contra redes de sensores inalámbricos basados en *malware* [56], [57], también se pueden dar otro tipo de ataques que no requieren tanta complejidad y que han demostrado ser realmente efectivos tanto desde un punto de vista práctico como teórico [58], [59], [60], [61], [62], [63]. Estos ataques no basados en *malware* o software complejo han conseguido degradar el desempeño y funcionalidades de la red, dejando patente que puede lanzarse en una red de sensores inalámbricos, independientemente de la complejidad y capacidad de procesamiento de los nodos. Por lo tanto, las limitaciones de los nodos y la existencia de amenazas específicas, presentan una serie de desafíos tanto en la implementación de las propias redes, como en la de los mecanismos y contramedidas de seguridad necesarias, para cubrir los objetivos y requisitos de Ciberseguridad deseados.

La seguridad de la información o Ciberseguridad consiste en la protección de la información, así como de los sistemas asociados, contra el acceso, uso, divulgación, interrupción, modificación o destrucción no autorizados [64]. El objetivo principal es cumplir con los siguientes requisitos de seguridad: (a) *Integridad*, que significa proteger la información contra su modificación o destrucción indebida, e incluye garantizar su no repudio y su autenticidad; (b) *Confidencialidad*, que significa preservar las restricciones de acceso autorizado y divulgación de la información, incluidos los medios para proteger la privacidad personal y la propiedad; y (c) *Disponibilidad*, que significa asegurar el acceso, uso oportuno y confiable de la información [64].

Por lo tanto, estos requisitos básicos de seguridad, que pueden ser aplicables a cualquier sistema de comunicaciones, son también pilares fundamentales en el caso de las redes de sensores inalámbricos [65], [66], [67].

- 1) La *confidencialidad* es un requisito de seguridad básico para mantener el secreto de los datos transmitidos entre los nodos, o entre estos y el nodo

coordinador de red. Este servicio garantiza que los datos sólo sean accesibles para aquellos dispositivos autorizados –dentro o fuera de la red– impidiendo su divulgación a dispositivos no autorizados. Una solución estándar para asegurar la confidencialidad de los datos es el uso de sistemas de encriptación, debiendo tener en cuenta las limitaciones de recursos de los nodos a la hora de su implementación [66].

- 2) La *integridad* es un servicio de seguridad cuyo objetivo es garantizar que los datos transmitidos no han sido modificados o alterados, ya sea de forma intencionada o accidental, en el proceso de transmisión. De hecho, este servicio se centra en evitar que un atacante pueda modificar los datos y generar, por ejemplo, lecturas erróneas en los nodos. Además, la integridad tiene como objetivo evitar que alteraciones accidentales en la transmisión, puedan provocar la recepción de datos erróneos en otros nodos o en el nodo coordinador [65].
- 3) La *disponibilidad* es un servicio de seguridad muy importante dentro una red de sensores inalámbricos ya que su objetivo principal es garantizar el acceso a los datos generados por los nodos cuando sea necesario. Este servicio se vuelve crítico en redes de aplicación industrial, donde se ejecutan tareas de monitorización, automatización, seguridad o control, que requieren la recopilación de datos en tiempo real. Los ataques de denegación de servicio (*Denial of Service*, DoS) representan una de las amenazas más serias contra la disponibilidad ya que estas redes se basan en la cooperación entre nodos para crear rutas de comunicación inalámbricas. Estos ataques, pueden ejecutarse en cualquier capa de comunicación del protocolo de red utilizado. Entre algunas de las medidas que se adoptan para conseguir el objetivo de la disponibilidad, se encuentra el uso de protocolos de encaminamiento robustos que permitan reconfiguraciones de rutas dentro de la red y la doten de resiliencia frente a ataques [67].

Además de estos requisitos, una red de sensores inalámbricos también ha de cumplir otra serie de aspectos relacionados con la Ciberseguridad. Por ejemplo, los servicios de *autenticación* y *autorización* son fundamentales para garantizar la identidad de los nodos que participan en la transmisión de los datos, y que sólo los nodos autorizados pueden acceder a los servicios o los recursos de la red. En el proceso de

comunicación entre nodos, cada nodo debe verificar y validar la legitimidad del nodo del que recibe los datos, así como la legitimidad del nodo al que se los envía. Sin un servicio de autenticación y autorización, los atacantes podrían falsificar las identidades de los nodos para difundir datos falsos o erróneos a través de la red inalámbrica, o incluso hacer que los nodos rechacen los datos recibidos al considerarlos no autorizados. Además, a medida que se implementan nuevos nodos o que se reponen nodos averiados o con fallos, hay que garantizar la difusión segura de esta información a otros nodos de la red, para evitar que un adversario pueda utilizar identidades antiguas. Otros requisitos de Ciberseguridad pueden comprender además la *localización segura* de los nodos, ya que, en muchas situaciones, es necesario ubicar con precisión y automáticamente cada nodo de sensor, la *actualización de los datos*, que garantice que éstos son recientes y que ningún atacante pueda reproducir mensajes anteriores o la *sincronización de tiempo* [67].

En definitiva, la consecución de uno o varios de estos requisitos de Ciberseguridad exige el diseño e implementación de medidas, que tengan en cuenta no solo las posibles amenazas contra estas redes, sino que también cumplan con los requisitos debidos a las limitaciones de recursos de los nodos. Como resultado, la Ciberseguridad en redes de sensores inalámbricas ha de buscar el equilibrio entre lo que se requiere, lo que es deseable y lo que se puede lograr de manera realista, debiendo por tanto marcar un objetivo de qué requisito de Ciberseguridad es realmente indispensable, y con qué tipo de servicio de seguridad puede alcanzarse.

3.2 Clasificación de las amenazas y ataques contra redes de sensores inalámbricos

Debido a los requisitos de despliegue de las redes de sensores en entornos agresivos o desatendidos, a la naturaleza abierta e inalámbrica del canal de comunicación utilizado, y a las limitaciones en los recursos de los nodos, tales como su capacidad de procesamiento y fuente de alimentación, convierten a estas redes en mucho más vulnerables frente a amenazas y ataques que el de cualquier otro tipo de redes. En la mayoría de los casos, la probabilidad de que un ataque pueda comprometer alguno de los requisitos de Ciberseguridad antes mencionados es mucho mayor en estas redes que en una red inalámbrica tradicional o que en una red cableada. En este sentido,

con respecto a la Ciberseguridad en las redes de sensores inalámbricos, pueden identificarse un número importante de amenazas y vectores de ataque, que capaces de sacar partido de las vulnerabilidades existentes en estas redes.

Las amenazas y ataques pueden clasificarse siguiendo diversos criterios, por ejemplo, según la naturaleza del atacante, pudiendo ser amenazas y ataques internos o externos; según la intención del atacante, pudiendo ser pasivos o activos; según las capacidades del dispositivo utilizado para realizar el ataque; o según el o los requisitos de seguridad que se quieren comprometer (integridad, confidencialidad disponibilidad, autenticación, etc.); o dependiendo del tipo de actuación que se realice sobre los datos (modificación, eliminación, etc.). Para el desarrollo de esta tesis, y en aras de facilitar la clasificación de ataques, se emplea el modelo de referencia basado en capas para Interconexión de Sistemas Abiertos (*Open Systems Interconnection*, OSI). Partiendo de este modelo conceptual, se pueden analizar los distintos tipos de ataques contra diversos protocolos de comunicación, dentro de los cuales destacan, por ser los más ampliamente utilizados en redes de sensores inalámbricos, el IEEE 802.11 (*Wireless Local Area Networks*, WLAN), IEEE 802.15.1 (*Bluetooth*) o IEEE 802.15.4 (*Wireless Personal Area Networks*, WPAN).

En los apartados siguientes se describen a modo de resumen, diferentes tipos de amenazas y ataques, para, posteriormente, realizar una clasificación más exhaustiva basada en la capa del protocolo en el modelo OSI objeto del ataque.

3.2.1 Amenazas y ataques según las características del atacante

En una primera división, según las capacidades del atacante las amenazas pueden catalogarse como externas e internas; además, las amenazas también se pueden diferenciar según el tipo de dispositivo utilizado.

3.2.1.1 Amenazas externas e internas

Las amenazas externas a una red de sensores inalámbricas proceden de nodos de fuera de la red, mientras que las amenazas internas provienen de nodos que aun formando parte de la red y siendo aparentemente legítimos, han sido comprometidos por el atacante para que actúen contra la propia red [66]. La existencia de nodos

comprometidos es una de las principales vulnerabilidades en las redes de sensores inalámbricos. Una vez que el atacante toma el control del nodo, éste puede lanzar un ataque interno, por ejemplo, deshabilitando los nodos comprometidos o ejecutando código malicioso en nodos que son miembros válidos de la red. En este caso, el atacante puede tener además acceso a alguna de las claves criptográficas utilizadas en la red. Por lo tanto, los ataques internos son difíciles de detectar y prevenir, lo que aumenta los desafíos de Ciberseguridad.

En un ataque externo el nodo o dispositivo atacante no pertenece a la red, aunque puede influir activamente en el canal de comunicación. Los ataques externos pueden dividirse en dos categorías: pasivos y activos. Los ataques externos pasivos suelen limitarse únicamente a la escucha clandestina del canal radio (*eavesdropping*), con el fin de interceptar el tráfico de la red. Generalmente, el atacante externo no dispone de conocimiento sobre los mecanismos de seguridad que se utilizan en la red, por lo que la escucha clandestina puede permitirle analizar los datos obtenidos y conocer información relevante sobre claves y protocolos de seguridad utilizados. Una amenaza externa pasiva, puede degenerar en ataque externo activo si el adversario dispone de suficiente conocimiento sobre la red a atacar. Un atacante en estas circunstancias podría proceder a la inyección de datos falsos, o bien a la manipulación los datos que circulan por la red, ya sea modificándolos, retransmitiéndolos, o provocando su rechazo por parte de otros nodos [67]. El objetivo principal de estos ataques suele ser comprometer alguno o todos los requisitos de Ciberseguridad de la red de sensores inalámbricos.

Dentro de los tipos de ataques activos, ya sean externos o internos, caben destacar la familia de los ataques de Denegación de Servicio DoS (*Denial of Service*). Un ataque DoS se define en su forma más clásica, como un evento que puede disminuir o eliminar la capacidad de una red para realizar su función esperada [68]. Este tipo de ataques representan un problema muy serio cuando se implementan redes de sensores inalámbricos para aplicaciones que requieren la entrega de datos críticos en tiempo real, como, por ejemplo, en entornos industriales o en aplicaciones de monitorización de infraestructuras. Además, como se verá posteriormente, este tipo de ataques pueden darse en cualquier capa del protocolo de comunicaciones utilizado.

3.2.1.2 Ataques y amenazas según el tipo de dispositivo utilizado

Los ataques y amenazas también pueden clasificarse de acuerdo con el tipo de dispositivo utilizado por el atacante y, especialmente, por los recursos de los que dispone el nodo malicioso. Normalmente, un atacante puede utilizar dos tipos de dispositivos como nodos comprometidos, ya sean con las mismas características que los nodos sensores de la red a atacar; o bien utilizar dispositivos más potentes en términos de ancho de banda, velocidad de procesamiento, capacidad de memoria, cobertura de radio y fuente de alimentación.

En el primer caso, un atacante puede desplegar un dispositivo de red con las mismas capacidades que los nodos sensores, ya sea introduciendo nodos sensores similares en la red a atacar o capturando nodos sensores de la red para su posterior reprogramación. La principal ventaja del primer método es su rapidez y facilidad de ejecución. Sin embargo, el segundo método tiene algunas limitaciones. En primer lugar, no es fácil capturar y reprogramar nodos de sensores automáticamente. En segundo lugar, en algunas aplicaciones, el entorno de despliegue hace que sea difícil o incluso imposible para los atacantes capturar nodos de sensores [69].

La segunda alternativa para lanzar un ataque es que el adversario pueda desplegar nodos mucho más potentes que los que conforman la red a atacar, como por ejemplo un ordenador portátil, una Tablet un Smartphone, o incluso un Dron, equipado con un transceptor de radio apropiado, que pueda transmitir a un nivel de potencia mucho más elevado y con mayor alcance que los nodos sensores de la red a atacar. En estas circunstancias, el adversario podría utilizar, por ejemplo, varios nodos portátiles para comunicar con los nodos sensores, y descubrir los mecanismos de seguridad empleados para, posteriormente insertar códigos maliciosos y comprometer varios nodos de la red sin necesidad de acceder a ellos físicamente ni moverlos de sus posiciones [69]. Esta opción abre muchas más vías de ataque debido al mayor disponibilidad de recursos del nodo atacante, en términos de suministro de energía, capacidad de procesamiento y de memoria, y potencia de comunicación, entre otras. Más aún, este tipo de actividades para comprometer a los nodos, pueden ejecutarse en todo momento ya que pueden implementarse automáticamente, siendo además difíciles de detectar [69]. La implementación de defensas contra esta clase de amenazas puede

resultar complicada, y representa una de las principales dificultades cuando se trata de garantizar los requisitos de Ciberseguridad en una red de sensores inalámbricos.

3.2.2 Clasificación de ataques según la capa objetivo del protocolo OSI

Si bien, como se describió en el Capítulo 2 –dentro del apartado sobre protocolos de comunicaciones en redes– no existe una arquitectura estándar basada en capas para los protocolos de comunicación utilizados en la implementación de las redes de sensores inalámbricos, una arquitectura de red basada en capas puede mejorar la robustez al circunscribir las interacciones y las interfaces de las capas. Uno de los criterios más ampliamente extendidos para la clasificación de ataques contra redes de sensores inalámbricos es categorizarlos según la capa del protocolo OSI objeto del ataque. En el Capítulo 2 se presentó de forma esquemática las capas del protocolo OSI y la funcionalidad que desempeñan cada una de ellas.

Según esta clasificación, cada capa puede considerarse vulnerable a diferentes ataques y, por lo tanto, se le pueden aplicar diferentes mecanismos de seguridad. Sin embargo, algunos tipos de ataques pueden no solo afectar a una capa concreta, si no que pueden propagarse a través de múltiples capas aprovechando las interacciones entre ellas.

3.2.2.1 Ataques contra la Capa Física

Algunas de las funciones principales que desempeña la capa física (PHY) dentro de la arquitectura de protocolos de comunicación es la transmisión y recepción de datos utilizando un determinado canal de radio y según a una técnica específica de modulación y difusión [70]. Dentro de esta capa, pueden darse dos tipos de ataques principalmente, el ataque de interferencia o *jamming* y el ataque de manipulación o *tampering*.

El ataque *jamming*, en el sentido más clásico, se considera un tipo de ataques DoS en el que el adversario intenta interferir con la frecuencia de radio utilizada por los nodos sensores, mediante la transmisión de una señal radio –generalmente de alta potencia– en la misma banda de frecuencia utilizada por la red objetivo. El dispositivo atacante puede iniciar ataques de interferencia estratégicos dirigiéndose a áreas

sensibles de la red, por ejemplo, al nodo coordinador de red, sin llamar la atención ya que la señal de interferencia que cumple con los estándares de la red [67]. Estos ataques pueden realizarse, además, de forma continuada o aleatoria. Dada su importancia para el desarrollo de esta tesis, el ataque *jamming* se discutirá en mayor profundidad en un apartado específico de este mismo Capítulo

En un ataque de *tampering*, el atacante captura un nodo sensor y con la intención de comprometer su seguridad realizando modificaciones sobre éste, tales como la alteración de componentes hardware, y/o software. La captura física del nodo también permitiría al atacante extraer información relevante sobre el dispositivo y sobre la propia red, obteniendo, por ejemplo, la dirección MAC de la capa de enlace de datos (*Data Link*), las claves de encriptación utilizadas, o el código del programa almacenado dentro del nodo. Esta información podría utilizarse más tarde para desencadenar otros tipos de ataques. Por ejemplo, el atacante puede manipular el nodo capturado mediante la instalación de un nuevo código que provoque, un comportamiento anómalo del sensor comprometido; también podría controlar el nodo y ejecutar acciones como alterar los servicios de encaminamiento, crear paquetes de datos duplicados, etc. [65]. En estas condiciones, el atacante podría incluso fabricar nodos comprometidos e ir integrándolos directamente en la red. Las redes de sensores inalámbricos son muy vulnerables a los ataques físicos, ya que a menudo éstas se despliegan en entornos desatendidos.

3.2.2.2 Ataques contra la capa de Enlace de Datos o de Control de Acceso al Medio

La capa de Enlace de Datos (*Data Link*) o de Control de Acceso al Medio (*Medium Access Control*, MAC) representa la interfaz entre la capa física y las capas superiores del protocolo, garantizando una adecuada comunicación. Esta capa es responsable de la multiplexación de datos, la detección de errores, la prevención de colisiones entre paquetes, y la retransmisión de datos [71]. Las principales amenazas y ataques en esta capa incluyen la generación de colisiones, las peticiones de conexión reiteradas, y la reproducción de paquetes entre otros. Una colisión se produce cuando dos o más nodos intentan transmitir simultáneamente, provocando el descarte de los paquetes de datos y su posterior retransmisión. Un atacante puede causar colisiones de forma intencionada seleccionando paquetes de datos específicos, como por ejemplo los mensajes de control de reconocimiento ACK (*ACKnowledge*). El atacante también

puede intentar de generar colisiones y afectar seriamente el protocolo de comunicación mediante la transmisión continua o aleatoria de mensajes (*jamming*). En todos estos casos, la generación repetida de colisiones puede utilizarse para provocar el agotamiento de los recursos [68]. De forma resumida podemos incluir los siguientes ataques contra la capa de enlace de datos.

Los *ataques de colisión* pueden considerarse como un tipo de ataque *jamming* contra la capa de enlace. Su objetivo es provocar colisiones mediante el envío de paquetes que generen ruido en el canal inalámbrico de la red. Estos ataques pueden ejecutarse con relativa facilidad utilizando un nodo comprometido. Por ejemplo, en el protocolo SMAC [72], un nodo atacante verificaría el canal de comunicación para asegurarse de que el canal está ocupado, recibiendo paquetes de control de flujo de la capa MAC, tales como RTS (*Ready To Send*) y CTS (*Clear To Send*). Si es así, entonces este nodo enviará paquetes corruptos para provocar colisiones con los paquetes legítimos que circulan por la red [67].

Los *ataques de difusión (broadcast)*, se producen cuando el nodo atacante disemina tráfico no autenticado en la red, pero siguiendo las reglas de la capa MAC. Estos mensajes han de ser recibidos y procesados por todos los nodos de la red antes de que sean rechazados, debido por ejemplo a una autenticación incorrecta del nodo o a un error en la suma de comprobación (*checksum*). El atacante también podría bombardear a los nodos con mensajes legítimos. Sin embargo, el propósito de estos mensajes sería el agotamiento de las baterías de los nodos, ya que evitaría que los nodos entrasen en modo de suspensión (*sleep*) o de reserva de energía, y los mantendría en modo activo, realizando continuamente funciones no necesarias [67].

Los *ataques de acceso continuo al canal o agotamiento*, pertenecen a los tipos de ataques de denegación de servicio (DoS), y tiene como objetivo principal agotar las baterías de los nodos para reducir la vida útil de la red. Básicamente, el ataque consiste en interrumpir el protocolo MAC, inyectando continuamente paquetes innecesarios en la red. La solicitud o transmisión continuada de datos a través del canal radio, conllevará el desperdicio de energía de los nodos en retransmisiones innecesarias [67]. Este ataque, al igual que los *ataques de colisión*, puede considerarse como un tipo de ataque *jamming* contra la capa de enlace.

Los *ataques de repetición (replay attack)*, se producen cuando los mensajes intercambiados entre los nodos sensores se registran y retransmiten para que se agote la

energía de los nodos receptores. Sin un mecanismo anti-repetición, los datos retransmitidos pueden transmitirse a través de la red, provocando un desperdicio de energía en todos los nodos de retransmisión. La retransmisión no detectada tiene la ventaja adicional para el atacante de desviar la red de su propósito original [67].

Los *ataques de sincronización* tienen como propósito provocar problemas de sincronización a nivel de la capa MAC. Se trata de un ataque relativamente fácil de ejecutar, pero difícil de detectar, ya que el nodo malicioso respeta las reglas impuestas por el protocolo de comunicación. De hecho, cada nodo sensor mantiene un tiempo de activación que determina sus períodos de escucha y de reposo; tiempo que es intercambiado periódicamente con sus nodos vecinos para sincronizar sus relojes y formar un clúster virtual [67]. Esto les permite *despertarse* o cambiar al modo de suspensión (*sleep*) al mismo tiempo. Los tiempos de activación se actualizan intercambiando un paquete de sincronización SYNC. El paquete SYNC es muy corto e incluye la dirección del remitente y el tiempo de su próxima suspensión. Cuando un nodo recibe un paquete SYNC de un nodo que pertenece al mismo clúster virtual, recalcula su tiempo de reposo (promedio de su siguiente tiempo de reposo y el tiempo de reposo recibido) para sincronizarlo con el nodo remitente. Por lo tanto, el atacante puede hacer que el nodo objetivo permanezca *despierto* durante una fracción adicional del ciclo de escucha enviando un mensaje de sincronización comprometida. En consecuencia, el nodo atacado prolonga su tiempo de escucha en función de la duración del tiempo de suspensión comprometido extraído del mensaje de sincronización recibido [67].

Los *ataques de interrogación* (también denominados como *ataques de privación del sueño*) tienen como objetivo agotar las baterías del nodo atacado, manteniéndolo siempre activo y evitando que éste pase al modo de suspensión (*sleep*) o de conservación de energía. De hecho, el atacante interactúa con la víctima de una forma que parece legítima. Por ejemplo, un nodo malicioso podría enviar periódicamente solicitudes de datos RTS (*Ready To Send*) y obligando al nodo víctima a aceptar estas solicitudes CTS (*Clear To Send*) y haciendo que este nodo permanezca despierto esperando datos que nunca serán enviados por el nodo atacante [67]. Por tanto, el uso de este ataque puede reducir drásticamente el tiempo de las baterías del nodo atacado, e incluso el tiempo de vida de la propia red atacada si este ataque se llevase a una escala

importante. Además, este ataque puede ser difícil de detectar ya que se lleva a cabo solo a través de interacciones entre nodos que parecen legítimos [67].

Los *ataques de suplantación de identidad (spoofing)* se basan en la falsificación de la identidad de un nodo malicioso, para hacerse pasar por un nodo legítimo de la red. Debido a la naturaleza de transmisión de las comunicaciones inalámbricas, la identidad con la que un nodo se presenta en la red a este nivel –por ejemplo, la dirección MAC– está abierta a todos sus nodos próximos, incluidos en el caso de que los hubiese, los nodos atacantes; por lo que sin la protección adecuada, un adversario podría lanzar este tipo de ataques. Un ataque típico de suplantación de identidad MAC es el ataque *Sybil* [62], en el que un atacante presenta ilegalmente múltiples identidades MAC. Según la intención sea obtener acceso a la red permanecer oculto, un atacante puede falsificar la MAC como si fuese un sensor legítimo normal. Incluso podría llegar a suplantar a la propia estación base o nodo de agregación de red para obtener privilegios o recursos no autorizados de ésta [73]. Si el ataque tiene éxito, se podría tomar el control de toda la red. Los ataques de suplantación de identidad suelen ser la base de otros ataques entre capas que pueden tener consecuencias graves [73].

En general, los ataques descritos con anterioridad se caracterizan por provocar una sobrecarga en la operativa de los nodos, derivando tanto en una saturación del canal inalámbrico, como en el agotamiento de sus escasos recursos, especialmente de sus baterías. Estos ataques pueden enmarcarse mayoritariamente en el grupo de los ataques de denegación de servicio (DoS).

3.2.2.3 Ataques contra la capa de Red

Las redes de sensores inalámbricos se basan en la cooperación entre nodos para crear rutas de comunicación, siendo desplegadas de forma extensiva en un determinado entorno para realizar tareas de monitorización, automatización, seguridad, control. La función de la capa de red es la creación de rutas confiables y redundantes entre los nodos sensores y entre éstos y el nodo de agregación, de acuerdo con un determinado criterio denominado métrica, que se define en el protocolo de encaminamiento implementado. La capa de red de en una red de sensores inalámbricos es vulnerable a diferentes tipos de ataques como tales como la falsificación de información de

encaminamiento, el reenvío selectivo de paquetes, el ataque de sumidero, el ataque *sybil*, el ataque de agujero de gusano y la inundación por mensajes HELLO, entre otros.

El ataque de *reenvío selectivo de paquetes* (*selective forwarding*) se basa en la necesidad de retransmisión de información entre los nodos para crear las rutas dentro de la red inalámbrica. Los protocolos de encaminamiento asumen que los nodos retransmitirán fielmente todos los paquetes que pasan a través de ellos. Un atacante puede crear nodos maliciosos o comprometer a nodos de la propia red para descartar al azar algunos de estos paquetes, o bien para dar prioridad a la retransmisión de los propios mensajes [65].

El *ataque Sybil* se produce cuando un atacante utiliza un nodo que presenta múltiples identidades ante el resto de los nodos de la red inalámbrica; incluso el nodo atacante puede hacer creer al resto de nodos que está en varios lugares al mismo tiempo. Esta multiplicidad, puede inducir a error a otros nodos al creer que existen rutas utilizadas por nodos diferentes con respecto al nodo atacante, que es quien realmente utiliza estas rutas [74].

El *ataque de sumidero* (*sinkhole*) tiene por objetivo atraer todo el tráfico de red que circula por una determinada zona hacia un nodo comprometido. Para ello, el atacante posiciona tal nodo comprometido en el centro del área objetivo, creando una zona de influencia y atrayendo hacia ésta todo el tráfico destinado a los nodos próximos o al nodo de agregación. El atacante seleccionará un lugar para crear un sumidero donde pueda atraer la mayor cantidad de tráfico, posiblemente lo más cerca posible al nodo de agregación, de este modo el nodo malicioso pueda percibirse por el resto de la red como un nodo de agregación legítimo [74].

El *ataque de agujero negro* (*black hole*), puede considerarse uno de los ataques de encaminamiento más simple contra una red de sensores inalámbricos. En este tipo de ataque, el nodo atacante absorbe todos los paquetes que pasan a través de él, no reenviando, por tanto, ninguno los paquetes que recibe. Al negarse a reenviar cualquier mensaje que recibe, el atacante afectará a todo el tráfico que fluye a través de él. Por lo tanto, el rendimiento de una zona de la red inalámbrica, especialmente aquella que engloba a los nodos vecinos alrededor del atacante se verá reducido drásticamente [73]. Las diferentes ubicaciones del atacante inducen diferentes influencias en la red. Si el atacante se encuentra cerca de la estación base o nodo de agregación, es posible que todo el tráfico que vaya a la estación base tenga que pasar por el atacante. Obviamente,

los ataques de agujero negro en este caso pueden dañar seriamente la comunicación entre la estación base y el resto de la red, e impidiendo que ésta que la cumpla sus propósitos efectivamente. Por el contrario, si un nodo atacante se sitúa en los alrededores de la red inalámbrica, probablemente muy pocos nodos lo utilicen para comunicarse con otros nodos, por lo que el daño puede ser muy limitado [73].

El *ataque de agujero de gusano (wormhole attack)*, utiliza un nodo malicioso para interceptar los paquetes de datos de sus nodos adyacentes y los retransmite mediante rutas a través de varios saltos a otro nodo malicioso, que es responsable de retransmitir estos paquetes nuevamente. Esto puede distorsionar las distancias entre los nodos de la red y falsear el proceso de descubrimiento de nodos vecinos. Por lo tanto, un nodo sensor puede seleccionar un nodo remoto como su vecino más cercano y transmitirle sus datos, lo que resulta en un agotamiento rápido de los recursos y reduce la vida útil de la red [67]. Este ataque es también conocido como ataque de *tunelización* y puede considerarse como uno de los ataques más efectivos contra una red de sensores inalámbricos. Para su ejecución requiere al menos dos nodos maliciosos vinculados por un potente enlace de radio o por un enlace de cable. En un ataque de agujero de gusano, la información recibida por un nodo malicioso en un lado de la red se encapsula y retransmite para ser reintroducida por otro nodo malicioso en el otro lado de la red, revelando que el mensaje se origina en un nodo cercano [65]. La encapsulación se puede realizar de dos maneras.

- 1) Mediante la encapsulación de múltiples saltos con el objetivo de ocultar los nodos intermedios ubicados entre los dos atacantes para que las rutas a través del nodo malicioso parezcan más cortas, lo que facilita la creación de *sumideros* con protocolos que utilizan el número de saltos como métrica principal de selección de rutas, y
- 2) mediante la encapsulación mediante comunicación directa, en la que las rutas que atraviesan por los nodos comprometidos son más rápidas porque están compuestas por un solo salto y pueden usarse contra protocolos que utilizan la primera ruta descubierta y aquellos basados en la latencia de rutas [65].

El ataque de *inundación por mensajes HELLO* aprovecha la característica de un gran número de protocolos de encaminamiento que, utilizan paquetes de datos específicos de *saludo* o *Hello*, con el fin de establecer la relación de proximidad o la solicitud de conexión entre nodos vecinos. En este ataque, el adversario envía paquetes

Hello a uno o varios nodos de la red que se encuentran alejados de él. Los nodos que reciben estos paquetes *Hello* asumen que el nodo atacante está próximo a ellos, por lo que lo identifican erróneamente como uno de sus vecinos. Como resultado, los nodos atacados no podrán reenviar paquetes de datos cuando utilicen al nodo atacante para su próximo salto, ya que en realidad éste no está dentro del alcance del nodo remitente. El ataque se denomina de inundación ya que, en general, estos paquetes *Hello* falsos del atacante, podrían transmitirse constantemente a todos los nodos de la red con suficiente potencia [63]. En esta situación, todos los nodos legítimos de la red identificarán erróneamente al nodo atacante como su vecino y esto podría hacer que todos estos nodos envíen paquetes a un destino falso creado por el nodo atacante [63].

El ataque de *suplantación de reconocimiento* (*acknowledgement spoofing*) aprovecha el hecho de que varios algoritmos de encaminamiento para redes de sensores, utilizan paquetes de reconocimientos (ACK) implícitos o explícitos de la capa de enlace [74]. Debido al medio de transmisión inherente, un atacante puede falsificar los paquetes ACK de reconocimiento en la capa de enlace para los paquetes dirigidos a los nodos vecinos. Los protocolos que eligen el siguiente salto en función de problemas de confiabilidad son susceptibles a la falsificación de paquetes ACK. Al viajar a lo largo de dichos enlaces, esto dará como resultado la pérdida de paquetes [74].

El *sniffing* es un ejemplo de ataque de interceptación o escucha clandestina del canal inalámbrico o *eavesdropping*. En este ataque, el adversario emplaza un nodo en las proximidades de la red de sensores para capturar datos de forma clandestina. Los datos recopilados por el atacante pueden ser posteriormente analizados por éste, para identificar los nodos más críticos que conforman la red. Por ejemplo, un aumento repentino en la cantidad de mensajes intercambiados entre los nodos sensores significa que representa actividades y eventos específicos que deben monitorearse. Además, el atacante puede identificar los nodos de agregación del clúster sin tener que comprender el contenido de los mensajes [67].

A grandes rasgos, los ataques descritos con anterioridad se caracterizan por provocar errores de comunicación entre los nodos, lo que en muchos casos derivará en de un ataque de denegación de servicio (DoS). Otra característica particular de estos ataques, es que suelen ser los precursores de ataques a las capas superiores, ya que en esta situación, el atacante dispone de un acceso bien consolidado a la red inalámbrica.

3.2.2.4 Ataques contra la capa de Transporte

La función principal de la capa de transporte es el de establecer conexiones punto a punto entre nodos, así como garantizar la entrega confiable de paquetes de datos entre ambos extremos de la comunicación. Además, en esta capa se implementan funciones de control de flujo y congestión de tráfico. La capa de transporte, puede utilizar protocolos de secuenciación para mejorar la fiabilidad de la conexión. Sin embargo, esto la hace muy vulnerable a los ataques de denegación de servicio [67]. Ataques como el de inundación (*flooding*), el de desincronización (*desynchronization*), o la replicación de nodos, entre otros son amenazas contra esta capa.

El *ataque de inundación (flooding)*, tiene como objetivo provocar una denegación de servicio (DoS) y reducir la vida útil de la red inalámbrica. Para su ejecución, el atacante puede emplazar uno o varios nodos maliciosos en la red, que propagarán gran cantidad de solicitudes de conexión de forma regular, a una potencia de emisión alta. Este ataque se producirá hasta agotar los recursos que requiere la conexión, o hasta alcanzar un límite máximo para saturar la red y evitar que nodos legítimos establezcan comunicaciones, lo que agotará sus recursos –memoria y energía– y reducirá la disponibilidad de la red inalámbrica [65].

El *ataque de desincronización (desynchronization)*, forma parte de los ataques de agotamiento de recursos. El atacante provoca la pérdida de tramas al distorsionar, cambiar o aumentar el número de secuencia de los paquetes intercambiados entre los nodos extremos de una comunicación. Al recibir los paquetes modificados, el nodo destino deduce que los paquetes se han perdido y solicita el reenvío de estos paquetes a los nodos remitentes, lo que interrumpe la sincronización de las comunicaciones y provoca un considerable desperdicio de energía de los sensores legítimos al intentar recuperarse de errores que nunca existieron realmente [65].

El *ataque de replicación de nodos*, es un ataque en el que el adversario intenta emplazar varios nodos con la misma identidad en diferentes lugares de la red existente. Hay dos métodos para ejecutar este ataque. En el primer método, el atacante captura un nodo de la red, crea clones del nodo capturado y los introduce en diferentes lugares de la red. En el segundo método, un atacante puede generar una identificación falsa de un nodo, para luego clonar este nodo e introducirlo en diferentes lugares de la red [74].

A parte de estos ataques, la capa de transporte es susceptible a ataques ya vistos con anterioridad, como el de agujero negro (*black hole*) o el de agotamiento de recursos. Además, otro tipo de ataque interesante contra esta capa es el *homing*. En este ataque, el adversario observa el tráfico de la red para deducir la ubicación geográfica de los nodos críticos, tales como como coordinadores de red o clúster, o los vecinos de la estación base. El atacante podría usar este ataque para deshabilitar físicamente estos nodos [74].

3.2.2.5 Ataques contra la capa de Aplicación

Como su propio nombre indica, la esta capa contiene las aplicaciones de usuario que realizan las funciones de monitorización, automatización, seguridad, control y en general cualquier otra tarea que requiera la recopilación de datos en tiempo real. Los atacantes suelen explotar las vulnerabilidades de los programas y aplicaciones que se ejecutan en los nodos sensores lanzando ataques tales como, la inyección de código, el desbordamiento de búfer o el acceso no autorizado a datos.

El *ataque de inyección de código* consiste en la introducción de código malicioso en el sistema mediante la explotación de errores de programa. Inyección de código se puede utilizar para una variedad de propósitos, por ejemplo, para robar datos, obtener el control del sistema y propagar gusanos. Este tipo de ataque puede hacer que el sistema pierda el control y comprometa la privacidad del usuario ante el atacante. o incluso a un apagado completo del sistema [76].

El *ataque de desbordamiento de búfer (buffer overflow)* implica la violación de los límites del código o búfer de datos mediante la explotación de las vulnerabilidades del programa. Muchos de los programas que se ejecutan en los nodos funcionan con un diseño de memoria predefinido que contiene segmentos de código y datos. El atacante podría escribir una secuencia de datos larga sobre un área de memoria específica, lo que resultará en desbordamiento de la secuencia más allá de su región de residencia predefinida [76]. El resultado puede ser la modificación de otros datos, por ejemplo, cuando la secuencia invade la región de datos de otro búfer de datos, ejecución de código malicioso, por ejemplo, invadiendo un segmento de código, y destrucción del flujo de control del programa. Además, ha habido demostraciones que muestran cómo este tipo de ataque puede permitir que un agente no autorizado obtener privilegios de administrador y ejecutar código arbitrario [76].

El *ataque de acceso no autorizado a datos* se basa en que una vez que el adversario obtiene los permisos de acceso necesarios a la aplicación ejecutada en el nodo, podría realizar cualquier operación de manipulación de datos, incluyendo la modificación o destrucción de éstos. Este ataque usualmente se aprovecha de vulnerabilidades en el diseño de los métodos de autenticación y gestión de permisos del usuario para el control de las aplicaciones. Hay constancia de atacantes que han sido capaces de explotar vulnerabilidades en el modelo de permisos para controlar aplicaciones en hogares inteligentes (*SmartHome*), causando problemas tales como allanamiento y robo [76].

Si bien estos ataques se consideran los más comunes contra los nodos de una red de sensores inalámbricos, la capa de aplicación también puede verse amenazada por virus, gusanos, troyanos; además, otros programas maliciosos que afectan a las redes y dispositivos convencionales también encuentran su lugar en esta capa, tales como los *rootkit*, *spyware*, *adware*, etc.

3.3 Sistemas y mecanismos de seguridad ante ataques contra redes de sensores inalámbricos

Como se mencionó anteriormente, las redes de sensores inalámbricos poseen una serie de características que hacen que este tipo de redes sean vulnerables a varios tipos de amenazas y ataques específicos. Por otro lado, las limitaciones en los recursos de los nodos, tales como su capacidad de procesamiento, fuente de alimentación, entre otras, hacen que la adopción de mecanismos de defensa contra ataques tradicionales, como los antivirus, el encriptado de clave simétrica, etc., sean inadecuados, por lo que abordar la Ciberseguridad para este tipo de redes resulta más complejo y plantea desafíos importantes tanto en diseño como en la implementación. En esta sección, se presentan varios de los mecanismos de defensa más habituales y relevantes utilizados para combatir la mayor parte de las amenazas y ataques contra las redes de sensores inalámbricos expuestos anteriormente.

3.3.1 Introducción

Uno de los mayores desafíos a los que se enfrenta la implementación de mecanismos de Ciberseguridad en redes de sensores inalámbricos es la limitación de los recursos disponibles en los nodos, debiendo alcanzarse un compromiso entre la minimización del consumo de recursos y la maximización de la seguridad. Por lo tanto, estos mecanismos de seguridad además de marcarse como objetivo proporcionar los requerimientos de confidencialidad, integridad, disponibilidad, etc., también han de respetar todas las limitaciones de recursos hardware y software de los nodos, tales como capacidad de batería, rango de transmisión de radio, ancho de banda, capacidad de procesamiento y memoria disponible, etc. Por una parte, los mecanismos de Ciberseguridad que adoptan enfoques de seguridad sólidos para proteger las redes de sensores pueden llevar al agotamiento de los recursos de los nodos. Por otra parte, los enfoques de seguridad livianos con un bajo consumo de recursos pueden no ser eficaces contra ciertos tipos de ataques, que pueden ir desde escuchas pasivas, hasta ataques activos de denegación de servicio que pueden afectar seriamente a redes que desempeñan funciones críticas. En consecuencia, siempre debe establecerse un equilibrio entre el nivel de Ciberseguridad proporcionado y el coste adicional introducido por la contramedida aplicada [67].

Teniendo en cuenta los tipos de ataques descritos anteriormente, así como los desafíos presentados, se han propuesto diferentes mecanismos de seguridad para redes de sensores inalámbricos, los cuales pueden dividirse en dos grandes grupos. Por una parte, se dispone de mecanismos de seguridad o contramedidas enfocadas a la prevención de ataques mediante el uso de sistemas de criptográficos, uso de claves y modelos de confianza; mientras que el otro grupo se centra en la detección de los ataques, como los sistemas de detección de intrusiones. Sin embargo, estos mecanismos por si solos no suelen ser capaces de hacer frente a ataques complejos, por lo que en ocasiones y siempre que la capacidad de la red lo permita, es preciso combinarlos para cumplir con todos los requisitos de seguridad, utilizando un enfoque clásico de Ciberseguridad, basado en la defensa en profundidad y la diversidad de defensas. Si bien en los últimos años se han publicado estudios exhaustivos en cuanto a los diferentes tipos de mecanismos, soluciones y contramedidas de seguridad aplicables a redes de sensores inalámbricos tales como [65], [67], [71], [73], [74], entre otros, en los

siguientes apartados se presenta un resumen de las soluciones más habituales y relevantes.

3.3.2 Mecanismos criptográficos

Los sistemas criptográficos son una de las contramedidas de seguridad más habituales que pueden encontrarse implementadas en los nodos de una red de sensores inalámbricos. El establecimiento de un mecanismo criptográfico basado en el uso de claves seguras permite realizar operaciones de encriptado y autenticación de los mensajes intercambiados entre los nodos sensores. La selección de un método criptográfico apropiado para los nodos sensores es fundamental para proporcionar los servicios de seguridad requeridos por la red, además de mantener la capacidad de comunicación de los nodos sensores. Por tanto, los algoritmos criptográficos deben respetar la limitación de recursos de los nodos sensores y no requerir una alta potencia de cálculo y capacidad de almacenamiento, además, deben ser energéticamente eficientes [67]. Por ejemplo, en muchas aplicaciones de redes de sensores, la implementación de una solución de criptografía asimétrica puede resultar demasiado costosa en términos de uso de recursos. Para solventar estas limitaciones, se han desarrollado alternativas criptográficas más eficientes.

3.3.2.1 Mecanismos criptográficos de clave simétrica

Los sistemas simétricos de encriptado son aquellos que utilizan la misma clave para cifrar y descifrar. Por lo tanto, la clave debe ser distribuida previamente a los nodos que vayan a utilizarla. La principal desventaja de esta solución es que la clave precargada en los nodos podría comprometer toda la red a través de nodos comprometidos. Una de las soluciones propuestas para superar este límite es establecer esquemas de encriptado simétrico basados en claves por pares en lugar de una única clave global [65].

Uno de los mecanismos de encriptado simétrico engloba a los protocolos de seguridad para redes de sensores desarrollado por [77] y denominado SPINs (*Security Protocols for Sensor Networks*), que utiliza dos bloques de construcción de claves seguros. Por un lado, se dispone de un protocolo de encriptado de red de sensores

(*Secure Network Encryption Protocol*, SNEP), el cual proporciona confidencialidad, autenticación y actualización de datos entre las dos partes de la comunicación con un consumo muy reducido de recursos. Por otro lado, SPINs incorpora una versión micro del protocolo de autenticación cronometrado, eficiente, de transmisión y tolerante a pérdidas denominado μ TESLA (*micro version of the Timed, Efficient, Streaming, Loss-tolerant Authentication Protocol*), que proporciona transmisión autenticada para entornos de red con serias limitaciones de recursos [77].

Los mecanismos criptográficos de clave simétrica utilizan una única clave compartida entre los dos hosts que se comunican, que se utiliza tanto para el encriptado como para el desencriptado. Sin embargo, un desafío importante para la implementación de la criptografía de clave simétrica es cómo distribuir de forma segura la clave compartida entre los dos hosts que se comunican. Este es un problema no trivial ya que la distribución previa de la clave no siempre es factible. En la sección siguiente se comentarán algunos mecanismos de distribución de claves habitualmente utilizados en las redes de sensores. Seleccionar el método criptográfico apropiado para los nodos sensores es fundamental para brindar servicios de seguridad en las en redes de sensores inalámbricos; sin embargo, la decisión depende de la capacidad de cálculo y comunicación de los nodos sensores [74].

3.3.2.2 Mecanismos criptográficos de clave asimétrica o clave pública

La criptografía asimétrica –también conocida como criptografía de clave pública– utiliza una pareja de claves denominadas *clave pública* y *clave privada*, de tal modo que el mensaje encriptado por la *clave pública* puede ser desencriptado por la *clave privada*. A modo de ejemplo, supóngase una comunicación entre dos nodos los cuales han distribuido sus claves públicas al través de la red inalámbrica. El nodo remitente utilizará la clave pública del nodo destino para cifrar un mensaje transmitido hacia éste, por lo que el nodo destinatario utilizará su clave privada para descifrar la información recibida, que ha sido cifrada por el nodo remitente. Este mecanismo de encriptación permite no solo el encriptado de la información, sino que también permite garantizar la autenticación de los nodos mediante el uso de firmas y certificados digitales.

La mayoría de los esquemas de claves simétricas actuales para redes de sensores, se enfocan a la seguridad de la capa de enlace para las comunicaciones de un solo salto entre nodos, pero no la seguridad de la capa de transporte para las comunicaciones de varios saltos. Es poco probable que cada nodo sea capaz de almacenar una clave de capa de transporte para cada uno de los otros nodos en una red debido a la gran cantidad de nodos. Probar la autenticidad de las claves públicas es otro problema importante. Los algoritmos de clave pública como RSA (*Rivest, Shamir y Adleman*) son computacionalmente intensivos y generalmente ejecutan miles o incluso millones de instrucciones de multiplicación para realizar una sola operación de seguridad [74].

La mayoría de los mecanismos criptográficos de clave pública resultan costosos desde el punto de vista del uso de recursos de los nodos y de la red. Si bien estos son uno de los principales inconvenientes de la utilización de sistemas de clave pública, los mecanismos de criptografía asimétricos están comenzándose a usar cada vez con más frecuencia en las redes de sensores inalámbricos [65].

3.3.3 Protocolos de gestión de claves

La gestión de claves es un mecanismo crucial para garantizar la seguridad en los servicios y aplicaciones dentro de una red de sensores inalámbricos. El objetivo de un protocolo o mecanismo gestión de claves es establecer las operaciones de generación, regeneración y distribución de claves de manera eficiente, segura y confiable entre todos los nodos legítimos pertenecientes a la red. En términos generales, los desafíos que se presentan en la gestión de claves en una red de sensores inalámbricos se pueden agrupar en seis categorías: Distribución previa de claves, descubrimiento de vecinos, Establecimiento de claves de ruta de extremo a extremo, aislamiento nodos aberrantes, Re-codificación, y Latencia de establecimiento de claves. Dependiendo de la arquitectura de red desplegada, los esquemas de gestión de claves pueden implementarse de forma centralizadas o distribuida [74].

La distribución de claves es una de las fases críticas en el proceso de gestión de claves. Esta fase consiste en distribuir las claves criptográficas de forma eficiente y segura entre todos los nodos legítimos pertenecientes a la red. Se pueden distinguir tres modelos esenciales para la distribución de claves [67].

El *modelo de distribución de claves de red* consiste en utilizar una clave única compartida por todos los nodos de la red. Se trata de un modelo de distribución simple en el que se les implementa a los nodos una clave única antes de que sean desplegados en la red inalámbrica. Por tanto, este modelo utiliza muy pocos recursos ya que sólo requiere el almacenamiento de una sola clave, y permite una fácil colaboración entre los nodos vecinos. Además, el uso de una sola clave ofrece oportunidades de evolución y flexibilidad en el caso de agregar nuevos nodos. Por el contrario, este modelo es muy vulnerable y no tiene capacidad de recuperación. Por ejemplo, en el caso de que uno sólo de los nodos se vea comprometido, será necesario recargar una nueva clave en todos los nodos de la red, ya que el atacante podría encontrar la clave de seguridad y comprometer así toda la red [67].

El *modelo de distribución de claves de red pareadas*, consiste en compartir una clave solo entre un par de nodos de sensores. Por lo tanto, cada nodo está precargado con $N-1$ claves secretas, siendo N el número de nodos en la red. Este modelo de distribución permite una resiliencia perfecta porque el compromiso de un nodo no afecta la seguridad de los otros nodos. Sin embargo, requiere una capacidad de memoria significativa para almacenar las claves $N-1$, especialmente cuando el tamaño de la red es muy grande. Además, la adición de nuevos nodos resulta muy complicada ya que los nodos existentes no tienen las claves de estos nuevos nodos [67].

El *modelo de distribución de claves por grupo* combina las características de los dos modelos anteriores. Dentro de un grupo de nodos, las comunicaciones utilizan una única clave compartida para codificación de la información. Mientras que, para la comunicación entre grupos, se utilizan claves compartidas entre cada par de grupos. Por tanto, se mantendrá un equilibrio entre robustez, resiliencia, escalabilidad y coste de los recursos. Sin embargo, este sistema es difícil de implementar [67].

En los modelos de distribución previa de claves, uno de los grandes problemas es cómo cargar un conjunto de claves –denominado llavero– en la limitada memoria de cada nodo sensor [74]. A modo de ejemplo, uno de los protocolos de gestión de claves ampliamente utilizados en las redes de sensores inalámbricos es el protocolo de autenticación y encriptado localizado LEAP+ (*Localized Encryption and Authentication Protocol*) [78]. El protocolo está diseñado para admitir el procesamiento dentro de la red, mientras que al mismo tiempo restringe el impacto de seguridad que un nodo comprometido provocaría sobre la red más próxima a éste. El diseño del protocolo está

motivado por la observación de que los diferentes tipos de mensajes intercambiados entre los nodos sensores tienen diferentes requisitos de seguridad y que un solo mecanismo de encriptado no es adecuado para cumplir con estos diferentes requisitos de seguridad [78]. LEAP+ admite el establecimiento de cuatro tipos de claves para cada nodo sensor: una clave individual compartida con la estación base, una clave por pares compartida con otro nodo sensor, una clave de clúster compartida con múltiples nodos vecinos y una clave global compartida por todos los nodos en la red [78]. LEAP+ también admite la autenticación de fuente local (débil) sin excluir el procesamiento en la red. Este protocolo ha demostrado ser muy eficaz como contramedida a ciertos ataques sofisticados, tales como los ataques de inundación HELLO, los ataques de clonación de nodos y los ataques de agujero de gusano [78].

Aunque existen diversas arquitecturas para la gestión y administración de claves, ésta es un área en constante evolución dentro de los esquemas de seguridad para redes de sensores inalámbricos. Una amplia descripción de los diferentes esquemas propuestos para la gestión y administración de claves pueden encontrarse en referencias como [65], [66], [67], [71], entre otras.

3.3.4 Sistemas de gestión de confianza y autenticación

Una de las aplicaciones para redes de sensores inalámbricos de los mecanismos de encriptado descritos anteriormente son los sistemas de gestión de confianza y autenticación. Por un lado, cualquier sistema de gestión de confianza tiene que estar especialmente diseñado y preparado para responder a problemas específicos que pueden surgir en este tipo de redes, tales como la autonomía de gestión, la descentralización y la inicialización. La confianza de un nodo se calcula basándose en el algoritmo criptográfico que se aplica, las estadísticas de disponibilidad y la información de envío de paquetes sobre el nodo. Si la confianza calculada asociada con un nodo cae por debajo de un umbral, el nodo se considera inseguro y se evita en el proceso de encaminamiento [74].

Por otra parte, la autenticación es uno de los mecanismos de seguridad básicos en las redes de sensores inalámbricos. A menudo construida alrededor de un sistema criptográfico, la autenticación asegura que los datos o los paquetes de control tales como la información de encaminamiento, ubicación y administración de claves,

provengan de fuentes autenticadas [74]. Tradicionalmente, los protocolos de autenticación implementados en redes de sensores inalámbricos utilizan un mecanismo de encriptado denominado Código de Autenticación de Mensajes (*Message Authentication Code*, MAC) basado en criptografía de clave simétrica. Para ello, el nodo remitente genera una huella digital o código de autenticación utilizando la clave simétrica compartida con el nodo receptor. Cuando este último recibe el mensaje, calcula el código MAC con la misma clave y lo compara con el código MAC recibido. Si ambos códigos son idénticos, entonces se determina que la fuente del mensaje es auténtica [67].

Como ejemplo, el protocolo SPIN (*Security Protocols for Sensor Networks*) comentado anteriormente, es especialmente adecuado para redes de sensores jerárquicas, incorporando dos mecanismos de autenticación denominados SNEP y μ TESLA. El primer mecanismo permite la autenticación de comunicaciones entre pares de nodos, mientras que μ TESLA proporciona la autenticación de comunicaciones de difusión entre un grupo de nodos. Para ello, los nodos sensores deben contar con la ayuda de la estación base para transmitir los mensajes de autenticación, lo que representa una de las desventajas de este protocolo. Además, SPIN puede ralentizar aplicaciones que requieren actuar en tiempo real, ya que el proceso de intercambio del código MAC aumentará los retrasos en la comunicación. Por ejemplo, al usar μ TESLA, el nodo receptor debe esperar una cierta cantidad de tiempo antes de que pueda autenticar el origen de los mensajes recibidos [67].

Otro protocolo de autenticación ampliamente utilizado en redes de sensores inalámbricos basado en un mecanismo de autenticación que utiliza criptografía asimétrica es el denominado *Low Entropy Authentication Protocol* (LEA) [79]. En el proceso de autenticación, el nodo remitente firma los datos para ser transmitidos con su clave privada mediante la producción de una firma digital, siendo enviado toda esta información al nodo destino. Este último descifra la firma con la clave pública y la compara con los datos recibidos. En el caso de que sean idénticos, se valida la firma y el remitente se autenticará como nodo legítimo [67]. Sin embargo, LEA puede ser muy costoso en términos de espacio de almacenamiento, ya que el tamaño de la firma es proporcional al tamaño de los mensajes enviados. Por otra parte, LEA requiere una clave pública única para cada mensaje, lo que requiere que el receptor almacene una gran cantidad de claves públicas. Además, el uso de algoritmos asimétricos implica una

alta sobrecarga de computación y memoria de los nodos, lo que no es apropiado para redes de sensores inalámbricos [67].

Otro protocolo destacable es TinySec (*Tiny Security*) el cual se utiliza para garantizar la autenticidad, confidencialidad e integridad de los datos en las redes de sensores inalámbricos [80]. El objetivo de este protocolo es proporcionar un mecanismo de seguridad que no requiera alta potencia computación y memoria para los nodos, ni un uso excesivo del ancho de banda del canal inalámbrico. El protocolo TinySec se basa en el mecanismo de autenticación de código (MAC), que utiliza un sistema de criptografía simétrica. Sin embargo, comparado con los protocolos anteriores, el tamaño del código MAC es muy pequeño (4 bytes en lugar de 8 o 16 bytes), lo que reduce significativamente la sobrecarga de seguridad [67]. El uso de este código simplificado puede satisfacer todos los requisitos de seguridad, mediante el uso de un mecanismo de control simple sobre el número de intentos de autenticación permitidos. Esto hace que un atacante deberá probar 232 combinaciones para encontrar el código correcto [67].

Una descripción de otros modelos de sistemas de gestión de confianza y autenticación pueden encontrarse en referencias como [65], [66], [67], [71], entre otras.

3.3.5 Sistemas de detección de intrusos

Los mecanismos de seguridad que se han descrito en los apartados anteriores, tienen como objetivo evitar que un atacante que emplace un nodo dentro o en las proximidades de una red de sensores inalámbricos, pueda tener éxito al lanzar su ataque. Sin embargo, estos mecanismos por sí solos son insuficientes para garantizar una seguridad óptima en la red. De hecho, al igual que en otros entornos, en este tipo de redes es de aplicación el concepto de *defensa en profundidad*. Este concepto se basa en la aplicación de múltiples contramedidas de manera escalonada para lograr los objetivos de seguridad. En concreto, se trata de colocar capas que contengan diferentes tecnologías de seguridad heterogéneas contra los vectores de ataque comunes, lo que garantiza que los ataques que una tecnología no sea capaz de detectar o contener, sean detectados o contenidos por otra [81]. Por ejemplo, como se describió en el apartado de tipos de ataques, un nodo atacante puede programarse comprometiendo un nodo auténtico y desplegándolo en la red. El nodo atacante puede actuar dentro la red como un nodo legítimo utilizando toda la información capturada para anular las

comprobaciones de autenticación y descifrar toda la información codificada [67]. Por lo tanto, para garantizar un mayor nivel de seguridad, es necesario la implementación de una segunda línea de defensa adicional a los mecanismos criptográficos. Esta segunda contramedida puede implementarse mediante los sistemas de detección de intrusos (*Intrusion Detection Systems*, IDS).

A grandes rasgos, la función principal de un IDS es la monitorización de la red de sensores inalámbricos con el fin de detectar y alertar sobre posibles comportamientos y actividades sospechosas realizadas por los nodos. Si bien se han propuesto una gran cantidad de técnicas y mecanismos para los sistemas de detección de intrusos aplicados a las redes de sensores inalámbricos, en este apartado se proporciona una descripción de los esquemas IDS más relevantes.

Los enfoques tradicionales que se utilizan para la detección de intrusos se basan en la suposición de que existe una notable diferencia entre el comportamiento de un nodo legítimo, y otro malicioso. Para ello, el IDS realiza un análisis de las actividades llevadas a cabo por los nodos, de tal modo que, si una actividad no pertenece al conjunto de las actividades definidas como normales y esperadas, entonces se considera anómala o sospechosa. Según el modelo de análisis y verificación de intrusiones realizado por el IDS, éstos se pueden clasificar en *sistemas de detección basados en reglas*, *sistemas de detección de anomalías del comportamiento* y *sistemas de detección basados en especificaciones*. Los sistemas de detección basados en reglas engloban a mecanismos tales como detección por de uso indebido de recursos de la red, o la detección basada en firmas de ataques conocidos. Los sistemas basados en la detección de reglas se utilizan de forma genérica para detectar patrones de intrusión conocidos enumerados en una base de ataques [67]. Por otra parte, los sistemas de detección de intrusos basados anomalías del comportamiento se utilizan para la detección de nuevas intrusiones o ataques no enumerados. En comparación con los sistemas de detección de anomalías, los sistemas basados en reglas tienen una baja tasa de falsos positivos o detección errónea de intrusiones. Sin embargo, los sistemas basados en anomalías ofrecen una alta tasa de detección de nuevos ataques, en comparación con los basados en la detección de reglas. La tercera categoría de sistemas de detección de intrusos denominados sistemas basados en especificaciones es una derivación del sistema de detección de anomalías del comportamiento. Éstos adoptan el mismo principio de detección de anomalías del comportamiento, sin embargo, en vez de aplicar una

definición del modelo de forma automática, la definición de comportamiento anómalo se realiza mediante un algoritmo de aprendizaje. Esto simplifica el sistema de detección y reduce significativamente la tasa de detecciones de falsos negativos. En comparación con la detección basada en anomalías, esta técnica parece ser la más apropiada teniendo en cuenta las limitaciones de recursos antes mencionadas de las redes de sensores inalámbricos [67].

Independientemente del esquema de detección de intrusiones elegido, la integración de mecanismos de seguridad de este tipo adaptados a las limitaciones propias de las redes de sensores inalámbricos supone un desafío importante. Por una parte, como ya se vio en el Capítulo anterior, las redes de sensores generalmente están dedicadas a aplicaciones específicas y, por lo tanto, para cada una de estas aplicaciones hay que definir claramente lo que se consideran como comportamientos predecibles. Esto hace que no resulte práctico instalar e inicializar un esquema de detección de intrusiones sin disponer de un conocimiento y análisis previos de la aplicación antes de su implementación. Además, debido a las limitaciones de recursos ya conocidas tanto de los nodos sensores como de la propia red, la implementación de funciones como el aprendizaje automático, la detección de anomalías, etc., puedan resultar realmente costosas en términos de consumo de ancho de banda, capacidad de procesamiento, uso de memoria o batería. De hecho, el campo de los mecanismos de seguridad para redes de sensores inalámbricos, los sistemas de detección de intrusiones están en continua evolución, surgiendo investigaciones, nuevos enfoques y nuevas propuestas para solventar los problemas a las limitaciones mencionados. En las siguientes referencias se pueden encontrar una amplia descripción de diferentes esquemas propuestos para los sistemas de detección de intrusos [23], [82], [83], [84], [85], [86].

3.3.6 Otros mecanismos de seguridad

Los mecanismos de seguridad vistos hasta ahora suponen el grueso de las soluciones comúnmente adoptadas para proteger una red de sensores inalámbricos frente a ataques internos y externos. Sin embargo, existen otros mecanismos que pueden utilizarse en conjunción con las contramedidas antes mencionadas.

La *localización segura* de los nodos dentro de una red de sensores inalámbricos, es una contramedida para proteger a la red frente a la manipulación o robo de los nodos,

especialmente cuando se despliegan en entornos desatendidos. Por otra parte, el conocimiento de la posición de los nodos es además una parte esencial de muchas operaciones y aplicaciones de redes de sensores. En estos casos, los nodos sensores que reportan los datos monitorizados también deben reportar la ubicación desde donde se recopila la información y, por lo tanto, los sensores deben conocer su posición [74].

La *agregación segura de datos* garantiza que solo los miembros legítimos de un determinado grupo de nodos reciben los datos de difusión y multidifusión que les corresponden, para lo que se emplean mecanismos de autenticación y encriptación adecuados. Dado que las redes de sensores inalámbricos tienen restricciones de energía y un ancho de banda limitado, la reducción de las comunicaciones entre los nodos sensores y las estaciones base o nodos de agregación en el caso de la existencia de clúster, tienen un efecto significativo en la conservación de energía y la utilización del ancho de banda. Las redes de sensores agregadas sirven para este propósito, donde se aplican principalmente técnicas de multidifusión y difusión para reducir la sobrecarga de comunicación y gestión de enviar un solo mensaje a varios receptores [74]. Como se describió en el Capítulo anterior, la agregación o fusión de datos es un proceso en el que los nodos intermediarios denominados *agregadores* recopilan la información de su entorno, la procesan localmente y solo envían el resultado final. Este envío se realiza bien a los nodos vecinos para el siguiente salto, o bien las estaciones base o nodos de agregación como usuario final. Esta importante operación reduce esencialmente la cantidad de datos transmitidos a través de la red y, por lo tanto, prolonga su vida útil. Un atacante podría falsificar o presentarse como un nodo de agregación, o hacerse pasar por un nodo legítimo y enviar al nodo de agregación datos falsos. En ambos casos el resultado de los datos agregados será muy diferente al resultado real determinado por los valores medidos [74].

La *generación segura de rutas* tiene como objetivo garantizar la integridad, autenticación y disponibilidad de los datos que circulan por la red de sensores inalámbricos, algo que es fundamental en muchas de las aplicaciones de este tipo de redes. Los protocolos de encaminamiento son susceptibles a una serie de ataques según la naturaleza del protocolo, su aplicación y el entorno en el que se pretende utilizar el protocolo, por lo que estos protocolos deben diseñarse de forma segura para que sean capaces de imponer contramedidas cuando sea necesario [87]. Existen diferentes enfoques para garantizar la seguridad del encaminamiento siendo una de las

aproximaciones más extendidas el uso de protocolos específicos para redes de sensores inalámbricos, a los que se les dota de atributos de seguridad mejorados. Estos atributos de seguridad son los mecanismos que permiten a los protocolos de encaminamiento defenderse de las posibles amenazas en toda la red, para lo que se requiere el análisis detallado de todos los principales parámetros de encaminamiento, así como algoritmos de mantenimiento de topología utilizados [88]. Por ejemplo, LEACH (*Low-energy adaptive clustering hierarchy*), es un protocolo basado en clústeres que utiliza la rotación aleatoria para determinar qué nodo se convertirá en nodo de agregación y distribuir uniformemente la carga de energía entre los sensores de la red [89]. Este protocolo puede ser modificado para añadir funcionalidades de creación de rutas seguras, surgiendo variantes como *Secure LEACH* [90], *Lightweight Secure LEACH* [91], o *Specification based secure LEACH* [92], entre otros. Diferentes alternativas y enfoques también pueden encontrarse en [93], [94].

3.4 Ataques de interferencia contra redes de sensores inalámbricos

Tal y como se ha descrito previamente en este mismo Capítulo, existen una gran variedad de amenazas y ataques contra redes de sensores inalámbricos que pueden degradar su funcionalidad no solo en aplicaciones ya implementadas, sino también en nuevos paradigmas emergentes que tienden a consolidarse tales como la Industria 4.0 o la Internet de las Cosas (*Internet of Things*, IoT) entre otros. En este contexto, los *ataques de interferencia* (tradicionalmente conocidos como *jamming*) son un tipo de ataque, no basado en *malware* o programación compleja, que puede lanzarse para dañar una red de sensores inalámbricos, independientemente de la complejidad y capacidad de procesamiento de los nodos. Los ciberataques *jamming* o de *interferencia*, por tanto se enmarcan como ataques de tipo Denegación de Servicio (DoS), que pueden afectar a varias capas del protocolo de comunicaciones OSI objeto del ataque.

Desde el punto de vista funcional, las redes de sensores inalámbricos se caracterizan por hacer uso de la cooperación entre los nodos que la forman para crear rutas de comunicación inalámbricas. Los dispositivos utilizados en estas redes están limitados en cuanto a sus capacidades de procesamiento, de memoria o autonomía de sus baterías. Si bien estas limitaciones pueden considerarse como una barrera natural contra ataques que requieran cierta complejidad, como por ejemplo la inyección de

código, la propia naturaleza de la tecnología inalámbrica y del propio protocolo de comunicación utilizado, así como factores relacionados con el modo de despliegue de este tipo de redes, aumentan significativamente la probabilidad de ejecutar ataques tipo *jamming* cuyo objetivo es interferir intencionalmente el funcionamiento normal del medio inalámbrico, a nivel físico y de enlace de datos, saturando el canal mediante la inyección continua o aleatoria de paquetes de datos (con o sin sentido), causando anomalías y errores en la transmisión de información entre los nodos dentro de la red. Si bien algunos autores agrupaban los ataques *jamming* como ataques de bloqueo o interferencia en la capa física [95], de acuerdo con taxonomías propuestas recientemente, y en especial la propuesta por Lichtman [96], los ataques *jamming* se engloban dentro de la categoría de ciberataques y están generalmente relacionados con los ataques de denegación de servicio (DoS). En este sentido, si bien las capas superiores del protocolo de comunicaciones OSI utilizado pueden verse afectadas por este tipo de ataques, la capa física y la capa de enlace de datos (o acceso al medio), pueden considerarse mucho más vulnerables frente a estos ataques. Estas capas, son susceptibles a ataques como el *jamming*, que no requieren *malware* o una programación compleja en los nodos atacantes para provocar degradación de la comunicación y funcionalidades en la red inalámbrica, ya que, en estos casos, el atacante podría bloquear la comunicación por completo.

Los ataques *jamming* contra la capa física se centran en el envío de señales de radiofrecuencia en el mismo rango que el protocolo de red utilizado. Esto puede realizarse enviando bits aleatorios de forma continuada sin cumplir con los estándares de la capa MAC, o bien enviar un flujo continuo de paquetes [58]. El atacante también puede enviar la señal de interferencia en un formato periódico aleatorio para ahorrar energía en el nodo atacante. Las tres técnicas mencionadas anteriormente se consideran interferencias activas, ya que se puede detectar la interferencia. Sin embargo, en el bloqueo reactivo, los atacantes no bloquean el canal cuando está inactivo, si no que por el contrario se quedan a la espera hasta que detectan actividades en el canal, siendo este el modo más eficaz de ataque *jamming* en la capa física [58].

En cuanto a los ataques *jamming* contra la capa de enlace de datos, el objetivo del atacante es bloquear los paquetes de datos. Si bien estos ataques suelen ser más eficientes energéticamente son más complicados de ejecutar, pero a su vez son difíciles de detectar y de detectar. En algunos casos, el *jamming* contra la capa de enlace también

puede centrarse en la señal de control, como por ejemplo en los mensajes ACK. Para ello, dado que existen diferentes tipos de protocolos MAC, el atacante debe utilizar nodos que empleen el mismo protocolo en esta capa que el utilizado por la red a atacar [58]. Ejemplos prácticos de estos ataques pueden encontrarse en [60], [61], entre otros.

Un atacante puede, por tanto, utilizar varias estrategias con diferentes niveles de eficiencia, para llevar a cabo tales ataques contra las capas física (PHY) y de enlace de datos o de acceso al medio (MAC), siendo las estrategias más habituales: la generación continuada de bits en la capa física o paquetes a nivel de enlace de datos, a una determinada tasa (*jamming constante*); el envío de bits o paquetes de forma regular siguiendo el estándar de capa de enlace de datos (*jamming engañoso*); la generación aleatoria de bits o paquetes de datos (*jamming aleatorio*); y la generación de bits o paquetes de datos tan pronto como detecta la utilización del canal inalámbrico (*jamming reactivo*). A continuación, se describen con más detalle estos tipos de jamming.

3.4.1 *Jamming constante*

Los ataques de *jamming constante* (*constant jamming*) se caracterizan porque el atacante genera continuamente bits en la capa física o paquetes a nivel de enlace de datos a una determinada tasa, con el objetivo de bloquear por completo la comunicación entre los nodos de la red inalámbrica. Además, estos bits o paquetes, suelen ser aleatorios y sin sentido, no obedeciendo los procedimientos establecidos para la comunicación de la capa de enlace de datos. La mayoría de los protocolos de comunicación inalámbrica emplean alguna forma de control de acceso al medio (MAC) con detección de portadora para permitir que los dispositivos puedan realizar una transmisión sin que haya colisiones en el canal radio, es decir, pueden enviarse datos solo cuando el canal está inactivo [96]. Un ataque *jamming* de este tipo puede hacer que el canal se encuentre siempre ocupado por el nodo atacante, provocando que la transmisión del resto de nodos se retrase o incluso se cancele por completo. Ante esta situación, los nodos sensores no podrán ni enviar ni recibir datos a de otros nodos.

3.4.2 *Jamming* engañoso

A diferencia del *jamming* constate, los ataques de *jamming* engañoso (*deceptive jamming*) se caracterizan porque el atacante envía un flujo continuo paquetes a nivel de enlace de datos a una determinada tasa, pero con apariencia de datos legítimos. Esto es, los paquetes generados obedecen los procedimientos establecidos para la comunicación de la capa de enlace de datos o capa MAC, lo que significa que disponen de un encabezado de paquete legítimo, si bien su carga de información (*payload*) suele ser inútil o carecer de sentido para los nodos que la reciben [97]. Al igual que en el caso anterior, el objetivo de este ataque es bloquear por completo la comunicación entre los nodos de la red inalámbrica, aprovechando que los mecanismos de control de colisiones en la capa de enlace de datos solo permiten el envío de datos cuando el canal radio está inactivo.

Este tipo de *jamming* puede resultar muy dañino para la red además de ser difícil de detectar, ya que el atacante utiliza los mismos protocolos en la capa de enlace de datos que los utilizados por nodos legítimos; si bien la ejecución de este ataque requiere disponer de nodos *jammer* idénticos a los nodos a atacados, lo que requerirá un mayor esfuerzo por parte del atacante.

3.4.3 *Jamming* aleatorio

En los ataques de *jamming* aleatorios (*random jamming*) al atacante genera paquetes de manera regular a una tasa determinada durante un intervalo de tiempo t_j , para posteriormente volver a modo de reposo o suspensión (*idle* o *sleep*) durante otro intervalo de tiempo t_s . Durante el período del ataque, el nodo malicioso puede actuar como *constant jammer* o *deceptive jammer*. Además, el atacante puede ajustar los tiempos de ataque y de reposo, así como la tasa de datos generada para aumentar o reducir el nivel de agresividad del ataque, o bien para pasar desapercibido en la red. Un valor bajo de t_j y de tasa de datos generada provocará una actividad reducida por parte del nodo *jammer* y, como consecuencia, un ataque por ejemplo tipo DoS no se llevará a cabo constantemente [22]. Sin embargo, desde el punto de vista de los mecanismos detección y bloqueo –de estar implementados– contra este tipo de ataques, les resultaría difícil detectarlo, ya que sus efectos podrían confundirse o malinterpretarse como

interferencias normales debido al entorno inalámbrico, provocadas, por ejemplo, por otras redes y dispositivos inalámbricos que comparten el mismo ancho de banda [22]. Del mismo modo, valores altos de t_j y de tasa de datos generada, producirá un efecto más severo en la red inalámbrica, desembocando en un ataque DoS mucho más dañino. Si bien este ataque podría ser detectado fácilmente por los mecanismos de detección y bloqueo –de estar implementados–, este escenario puede considerarse como el peor de los casos para una red de sensores inalámbricos en términos de degradación del rendimiento [22].

3.4.4 *Jamming* reactivo

En el ataque *jamming* reactivo (*reactive jamming*), el atacante se aprovecha del mecanismo de control de acceso al medio (MAC) con detección de portadora que emplean la mayoría de los protocolos de comunicación inalámbrica. Teniendo en cuenta que el objetivo de estos mecanismos es evitar las colisiones en el canal radio y que sólo puedan enviarse datos cuando el canal está inactivo, la estrategia del atacante se basa en mantenerse a la escucha del canal hasta que detecta una transmisión en curso. En ese instante, el atacante emite un paquete de datos, provocando colisiones en el canal radio con los paquetes de datos legítimos. El atacante, puede entonces continuar monitorizando el canal, generando nuevas colisiones y actuando como *constant jammer* o *deceptive jammer* [22]. En el caso de que no se hayan implementado mecanismos de corrección de errores en la capa de protocolo afectada, o en las inmediatamente superiores, el ataque tendrá éxito con tan solo conseguir la alteración de un bit del paquete de datos legítimo. Por otro lado, si se dispusiese de tal mecanismo de corrección de errores, los efectos del ataque serían diferentes, aunque también perjudicarían al desempeño de la red. Por, ejemplo, el nodo destino detectaría el error y solicitarían nuevamente el reenvío del paquete al nodo remitente, lo que generará una gran cantidad de tráfico en el canal inalámbrico, además del uso de recursos extra por parte de los nodos [22].

Si bien este tipo de ataques suele ser muy sofisticado y requiere un conocimiento muy preciso de la configuración de la red a atacar a nivel de protocolos utilizados, también es quizás uno de los ataques más difíciles de detectar [98]. Esto se debe a que el nodo atacante permanecerá escuchando el canal de forma clandestina (*eavesdropping*)

hasta que detecte actividad en el canal, y proceda a generar los paquetes de interferencia. De ese modo, al igual que ocurría con el *jamming* aleatorio, los efectos provocados podrían confundirse con errores puntuales en la transmisión, o incluso.

3.4.5 Ataques *jamming* sofisticados

En los apartados anteriores se ha hecho referencia a los ataques *jamming* más comunes, que se pueden aplicar independientemente de los protocolos de encaminamiento utilizados, los mecanismos en las capas de acceso al medio, y en especial, de la complejidad de los nodos utilizados en la red inalámbrica. Sin embargo, existen otros tipos de ataques *jamming* mucho más sofisticados que pueden resultar de combinaciones de los anteriores o bien de añadir funcionalidades a los nodos atacantes, como por ejemplo el análisis de los protocolos de red o MAC para atacar a paquetes específicos, maximizando los efectos del ataque y minimizando el consumo de recursos de los nodos atacantes.

Por otra parte, los ataques *jamming* expuestos se centran principalmente en las primeras capas del protocolo de comunicaciones OSI, sin embargo, potencialmente pueden darse ataques *jamming* capas superiores. En estos ataques contra capas superiores, el objetivo son los paquetes y las tramas de control de las capas red y de transporte. El ataque *jamming* en capas superiores puede ser más eficaz, energéticamente eficiente y más difícil de detectar. Sin embargo, como contrapunto, podría ser más difícil y complicado de implementar [58]. Por ejemplo, un atacante puede interferir cada vez que los nodos intercambien paquetes y/o tramas de control para la actualización periódica de sus tablas de encaminamiento de las capas red y de transporte. Esta interferencia en las tablas de encaminamiento puede generar un problema grave para toda la red. Incluso en la capa de aplicación, un atacante puede interferir el canal inalámbrico de modo que bloquee, el establecimiento de conexión y la autenticación periódicas [58].

3.4.6 Descriptores estadísticos para la detección de ataques *jamming*

La presencia de nodos atacantes tipo *jammers* puede detectarse, evaluando diferentes métricas relacionadas con la calidad de la transmisión, ya sea en nodos

transmisores o receptores, que reflejan los efectos provocados por los ataques *jamming* expuestos hasta ahora. Básicamente, se trata de obtener estadísticas del tráfico de red. Un ejemplo de descriptores estadísticos utilizados habitualmente son la proporción de paquetes enviados (*Packet Sent Ratio*, PSR) y la proporción de paquetes entregados (*Packet Delivery Ratio*, PDR).

- 1) La proporción de paquetes enviados (PSR) refleja la proporción de paquetes que se envían con éxito por una fuente de tráfico legítima en comparación con la cantidad de paquetes que pretende enviar en la capa de enlace de datos o capa MAC [97]. La mayoría de los protocolos de comunicación inalámbrica emplean alguna forma de control de acceso al medio con detección de portadora para permitir que los dispositivos puedan realizar una transmisión sin que haya colisiones en el canal radio. Un ataque *jamming* puede hacer que el canal se encuentre siempre por el nodo adversario, provocando que la transmisión del resto de nodos se retrase. Esto puede provocar que un nodo almacene demasiados paquetes pendientes de enviar en la capa MAC, provocando que los paquetes recién llegados se descarten. También es posible que un paquete permanezca en la capa MAC durante demasiado tiempo, lo que dará como resultado un tiempo de espera elevado provocando también que los paquetes se descarten [97]. El PSR se define como m / n , siendo n el número de paquetes que el nodo tiene intención de enviar y m el número de paquetes que son realmente enviados. La medición del PSR se puede medir fácilmente con un dispositivo inalámbrico al realizar un seguimiento de la cantidad de paquetes que pretende enviar y la cantidad de paquetes que se envían con éxito [97].
- 2) Por otro lado, la proporción de entrega de paquetes (PDR), indica la proporción de paquetes que se entregan correctamente a un destino en comparación con la cantidad de paquetes que ha enviado el remitente [99]. Incluso después de que un nodo envíe el paquete, es posible que el nodo destino no pueda decodificarlo correctamente debido a la interferencia introducida por el nodo atacante, produciendo por tanto una entrega fallida. El PDR puede medirse en el nodo destino calculando la relación entre el número de paquetes que pasan la Comprobación de Redundancia Cíclica (*Cyclic Redundancy Check*, CRC) con respecto al número de paquetes o

preámbulos recibidos. El PDR también puede calcularse en el nodo remitente haciendo que el nodo destino envíe un paquete de confirmación. En cualquier caso, si no se reciben paquetes, el PDR se define como nulo [99]

3.5 Conclusiones

En este Capítulo, se han descrito los aspectos principales de la seguridad en redes de sensores inalámbricos, que comprenden los desafíos y obstáculos en su implementación, los requisitos de seguridad, los tipos de ataques, y los mecanismos y soluciones de defensas contra ataques. Así mismo, se han presentado los ataques típicos y se ha revisado en mayor profundidad el ataque tipo *jamming*, que será la base para la investigación presentada en esta Tesis. El objetivo de este Capítulo ha sido proporcionar una descripción general de los enfoques de seguridad existentes en las redes de sensores inalámbricos y destacar los problemas de seguridad que permanecen abiertos, pues aunque se han realizado esfuerzos muy importantes en el desarrollo de soluciones de seguridad tales como la criptografía, gestión de claves, la detección de intrusiones, la agregación segura de datos o el encaminamiento seguro, entre otras, todavía quedan algunos desafíos por abordar que requieren más actividades de investigación.

CAPÍTULO

4

Fundamentos de la Teoría Epidemiológica

Según la Organización Mundial de la Salud (WHO, *World Health Organization*) *la Epidemiología es el estudio de la distribución y los determinantes de los estados o eventos relacionados con la salud –incluidas las enfermedades–, y la aplicación de este estudio para el control de enfermedades y otros problemas de salud. Se pueden usar varios métodos para llevar a cabo investigaciones epidemiológicas: la vigilancia y los estudios descriptivos se pueden usar para estudiar la distribución; Los estudios analíticos se utilizan para estudiar los determinantes* [100]. En este mismo contexto la propia Organización define la enfermedad como un conjunto de disfunciones en cualquiera de los sistemas del cuerpo, definidos por una serie de manifestaciones con un patrón conocido de signos, síntomas y hallazgos relacionados, que además presenta una característica concreta de desarrollo a lo largo del tiempo dentro de una población [101]. Dentro de esta definición de enfermedad, se incluyen las enfermedades infecciosas, las cuales son causadas por microorganismos patógenos, como bacterias, virus, parásitos u hongos; estas enfermedades se caracterizan porque pueden transmitirse, directa o indirectamente, de una persona a otra. Además, las enfermedades zoonóticas son enfermedades infecciosas de los animales que pueden causar enfermedades cuando se transmiten a los humanos [102].

La teoría epidemiológica utiliza, por tanto, modelos matemáticos descriptivos para estudiar y analizar la dinámica de la propagación de enfermedades en una determinada población. En este sentido, se distinguen dos situaciones diferenciadas, una da origen al concepto de enfermedad endémica, que es aquella que persiste en el tiempo, y otra al concepto de epidemia que se define como un brote temporal de una enfermedad mayor de lo usual dentro de la población a estudio. Por lo tanto, un aspecto importante de la teoría epidemiológica es conocer si la enfermedad se detuvo debido a que ya no existían más individuos susceptibles dentro de la población, o bien por la influencia de factores, como la facilidad de transmisión del agente infeccioso, la recuperación de los infectados, la mortalidad, etc.

En este Capítulo se presenta un estudio sobre los modelos matemáticos más relevantes utilizados en epidemiología. Dentro amplio campo que representa la epidemiología, se ha incluido en este Capítulo una descripción de los modelos básicos pertenecientes al grupo de los modelos denominados *mecanicistas* definiendo, además, conceptos básicos propios de la epidemiología. Por otra parte, también se han incluido en este estudio los modelos epidemiológicos, denominados modelos *fenomenológicos*,

Señalar que, el desarrollo de los modelos epidemiológico objeto de esta Tesis se ha centrado en aquellos modelos que estudian las denominadas enfermedades infecciosas, ya que sus características de propagación (pueden ser transmitidas de un individuo a otro dentro de una determinada población, ya sea de forma directa o indirecta), hacen que la proximidad de un individuo sano a otro individuo infectado suponga un aumento significativo del riesgo o probabilidad de resultar también infectado. Este concepto de transmisión por proximidad en ausencia de contacto, se ajusta al modelo de comunicación inalámbrica utilizado en las redes a estudio.

4.1 Introducción

Si bien los primeros estudios matemáticos en epidemiología aparecieron en el siglo XVIII con el trabajo publicado en 1760 por el médico y matemático D. Bernoulli, la mayoría de los modelos epidemiológicos actuales derivan de los modelos matemáticos propuestos en 1927 por Kermack y McKendrick para describir epidemias en la India [103]. En estos modelos la población es dividida en grupos o compartimentos –de ahí que también se les denomine como *Modelos Compartimentales*– representando cada uno de ellos un estado con respecto a una determinada enfermedad (Susceptibles, Expuestos, Infectados, Recuperados, etc.). Para completar el modelo, se define la dinámica por la que los individuos dentro de la población pasan de un compartimento a otro teniendo en cuenta parámetros como la tasa de infección, el periodo de incubación o el período de recuperación de los individuos infectados. El análisis de estos parámetros permite obtener un valor umbral, para determinar si, en teoría, la enfermedad se extinguirá por si sola en la población (*Disease-free Equilibrium*, DFE), o si por el contrario se generará un brote epidémico de dicha enfermedad (*Endemic Equilibrium*, EE). Este brote epidémico, puede desaparecer al cabo de un tiempo más o menos prolongado, o bien permanecer durante largo tiempo entre la población, especialmente cuando existe una aportación continua de nuevos individuos susceptibles a dicha enfermedad, convirtiéndose entonces en una enfermedad endémica. Fueron Kermack y McKendrick los que postularon en su *teorema del umbral*, que la introducción de un individuo infectado en una población no provocará un brote epidémico salvo que la densidad de la población de individuos susceptibles supere un cierto valor crítico. Dicho valor umbral se denomina *Número Reproductivo Básico*, representado por \mathcal{R}_0 , y es uno de los parámetros fundamentales en el estudio de la propagación de enfermedades. Este valor umbral representa el número promedio de infecciones secundarias que ocurren cuando el primer individuo infectado (paciente cero) se introduce en una población de individuos completamente susceptibles. El valor de \mathcal{R}_0 dependerá de las características epidemiológicas de la enfermedad, y de las características demográficas y capacidad inmunitaria de la población. La teoría epidemiológica sostiene que si $\mathcal{R}_0 < 1$ la transmisión de la

enfermedad entre individuos será muy reducida y la enfermedad se extinguirá por sí sola en la población. Por el contrario, si $\mathcal{R}_0 > 1$ podemos esperar la aparición de un brote epidémico de dicha enfermedad dentro de la población, siendo este brote de mayor o menor intensidad dependiendo del valor de \mathcal{R}_0 . De esta manera, la teoría epidemiológica, y en especial \mathcal{R}_0 , puede utilizarse como herramienta para establecer tratamientos, estrategias y planes para la prevención y el control de enfermedades, tales como la vacunación o la cuarentena. Hay que destacar que, para una población y una enfermedad particulares, \mathcal{R}_0 suele tomar un valor constante dentro del intervalo de tiempo que dura la enfermedad [104]. Como ejemplo, en la Tabla 4.1 se presentan los valores de \mathcal{R}_0 de algunas enfermedades y epidemias conocidas.

Brote de enfermedad y localización	Fecha	\mathcal{R}_0	Referencias
Gripe española en Ginebra (brote otoño)	1918	3,8	[105]
Pandemia de gripe (H2N2) en USA	1957	1,68	[106]
Sarampión en Ghana	1960 a 1968	14,5	[107]
Viruela en el Subcontinente Indio	1968 a 1973	4,5	[107]
Epidemia de SARS (China, Hong-Kong)	2002 a 2003	3,5	[108]
Epidemia gripe (H1N1) en USA	2009	1,7 – 1,8	[109]
Ébola en Guinea	2014	1,51	[110]
Zika en Sudamérica	2015 a 2016	2,06	[111]
COVID-19 China	2020	2.24 – 3.58	[112]
COVID-19 España	2021	1,03 – 7,51	[24], [113]

Tabla 4.1. Valores de \mathcal{R}_0 para algunas enfermedades y epidemias conocidas.

En general, la obtención de \mathcal{R}_0 y la estimación de los parámetros de la enfermedad para el ajuste de las curvas de los modelos epidemiológicos resulta bastante complicado y puede diferir entre modelos, ya que en la mayoría de los casos los datos de una epidemia sólo pueden obtenerse una vez que esta concluye y, en ocasiones, estos datos obtenidos a posteriori pueden estar incompletos, contener irregularidades o ser inexactos.

En cualquier caso, dado que \mathcal{R}_0 es un parámetro clave para entender la dinámica de la propagación de una enfermedad y de su brote epidémico, se han propuesto

diversos métodos para su estimación [114], [115], [116], [117], entre otros, y en especial en sus etapas iniciales [118], [119], ya que es aquí donde se deben desplegar las medidas necesarias para la contención de la epidemia. Si bien en este mismo Capítulo se analizará con posterioridad como obtener \mathcal{R}_0 para el modelo objeto de esta tesis, a modo de introducción se presenta de forma resumida una serie de nociones sobre la formulación y características de \mathcal{R}_0 . Tal y como se indicó con anterioridad, el número reproductivo básico se interpreta desde el punto de vista epidemiológico como el número de casos secundarios esperados, producidos por un único individuo infectado introducido en una población completamente susceptible, siendo este valor un número adimensional. Desde el punto de vista matemático, puede expresarse como un producto de tres términos [120], $\mathcal{R}_0 = \tau \cdot \bar{c} \cdot d$, donde τ representa la transmisibilidad, esto es, la probabilidad de que se produzca una infección dado el contacto entre un individuo susceptible y un individuo infectado, \bar{c} es la tasa promedio de contacto entre individuos susceptibles e infectados, y d es la duración de la infección en el individuo infectado. En general los términos $\tau \cdot \bar{c}$ se agrupan en lo que se denomina tasa de infección o contagio, habitualmente identificada como β , mientras que el parámetro d , se utiliza el inverso del tiempo de recuperación del individuo frente a la infección.

4.2 Modelos epidemiológicos básicos

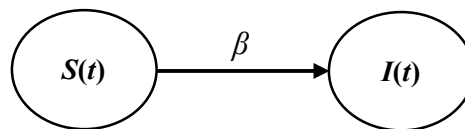
El primer conjunto de modelos epidemiológicos a estudio se basa en enfoques mecánicos o físicos para identificar patrones en los datos observados, por lo que son definidos como modelos *mecanicistas*. Los modelos matemáticos básicos más utilizados son el SI (Susceptible, Infectado), el SIS (Susceptible, Infectado, Susceptible), el SIR (Susceptible, Infectado, Recuperado), SEIS (Susceptible, Expuesto, Infectado, Susceptible), el SEIR (Susceptible, Expuesto, Infectado, Recuperado), entre otros. Estos modelos se diferencian, básicamente en el hecho de que los estados por los que pasa el individuo con respecto a la enfermedad pueden proporcionarle o no inmunidad ante futuros contagios de esa misma enfermedad. En todos estos modelos se considera que el tiempo en el que se produce todo el proceso de la enfermedad es suficientemente pequeño como para asumir que la población es constante durante dicho proceso

epidémico, no existiendo, por tanto, ni nacimientos ni fallecimientos de individuos. Por otro lado, todos estos modelos se basan en la Ley de Acción de Masas, donde se considera que, la velocidad de contacto entre de dos tipos individuos es aproximadamente proporcional al producto de las densidades de las respectivas subpoblaciones, siendo la constante de proporcionalidad una medida de la eficiencia de la transmisión de la enfermedad. Esta constante depende de factores, como la dinámica individual o demográfica, y de las condiciones ambientales, entre otras [104].

4.2.1 Modelos de enfermedades que no confieren inmunidad tras la infección

Cuando los individuos nunca se recuperan tras una enfermedad o ésta no les proporciona inmunidad permanente ante contagios futuros, se estaría ante modelos epidemiológicos del tipo SI y SIS respectivamente. Si además existe un periodo de latencia desde que se produce la infección hasta que la enfermedad comienza a presentar síntomas, entonces se trata de un modelo SEIS.

El modelo epidemiológico más simple es el SI, en el que la población está formada por dos únicos grupos de individuos, los Susceptibles y los Infectados, por lo que, si un individuo se contagia, la enfermedad será permanente en él. Su dinámica de propagación se presenta con los siguientes dos estados.



Siendo β la tasa de infección o contagio que representa la probabilidad de que un individuo susceptible enferme al estar en contacto con un infectado. El modelo, puede formularse para una población de N individuos con el siguiente sistema de ecuaciones diferenciales ordinarias, con $N = S + I$.

$$\frac{dS(t)}{dt} = -\beta SI, \quad \forall S(0) > 0 \quad 4.1$$

$$\frac{dI(t)}{dt} = \beta SI, \quad \forall I(0) > 0 \quad 4.2$$

La Figura 4.1 representa una simulación del modelo SI. Este modelo se aplicaba a enfermedades víricas como el VIH, donde la infección que causaba era vitalicia.

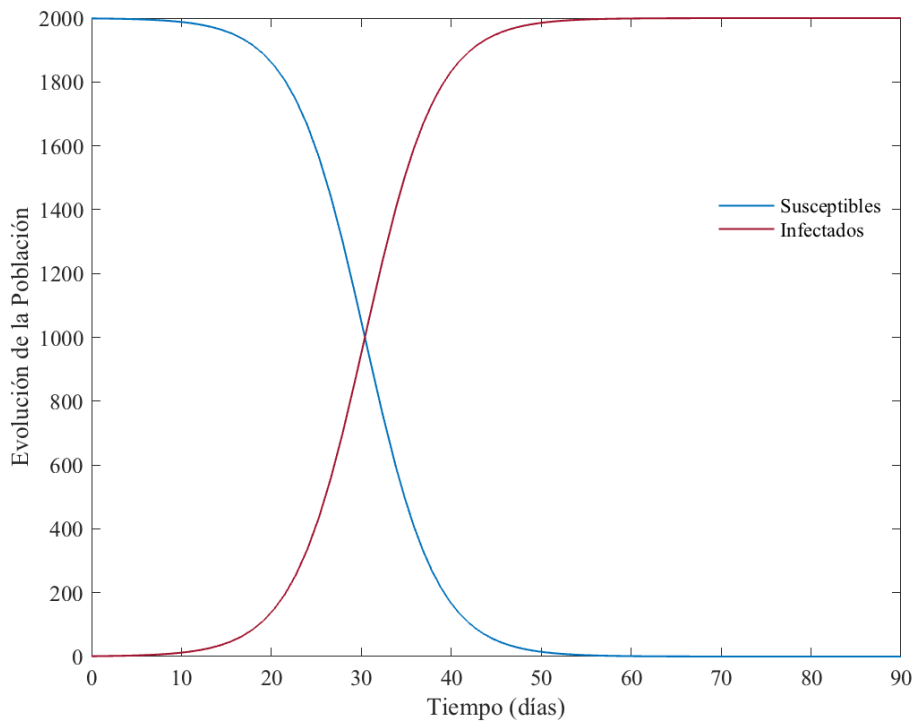
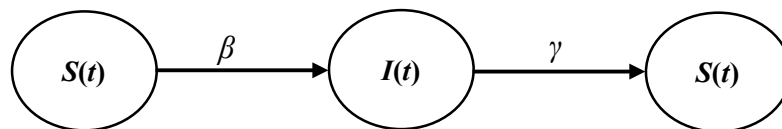


Figura 4.1. Simulación de la dinámica de una enfermedad para el modelo SI con una tasa de infección o contagio $\beta = 1.25 \cdot 10^{-4}$, con $S_0 = 1999$ e $I_0 = 1$.

Otro modelo básico es el denominado SIS, que también se aplica en casos en los que la enfermedad no confiere inmunidad a los individuos que se recuperan tras la infección, por lo que pasan nuevamente a ser susceptibles de contraer la enfermedad. Su dinámica de propagación se representa de modo que los individuos pasan del estado susceptible al de infectado y al recuperarse vuelven a ser susceptibles.



Al igual que en el modelo anterior, β representa la tasa de infección y depende de cada enfermedad y de ambas poblaciones; mientras que γ representa la tasa de recuperación siendo la duración de la infección $d = 1/\gamma$, que sólo depende de la población de individuos infectados que haya en cada momento. El modelo, puede formularse para una población de N individuos con el siguiente sistema de ecuaciones diferenciales ordinarias, con $N = S + I$ y $\mathcal{R}_0 = \beta N/\gamma$.

$$\frac{dS(t)}{dt} = -\beta SI + \gamma I, \quad \forall S(0) > 0 \quad 4.3$$

$$\frac{dI(t)}{dt} = \beta SI - \gamma I, \quad \forall I(0) > 0 \quad 4.4$$

La Figura 4.2 representa una simulación del modelo SIS. Este modelo se aplica a enfermedades que no confieren inmunidad tras la infección, como la meningitis, la peste, la malaria y algunos tipos de enfermedades de transmisión sexual.

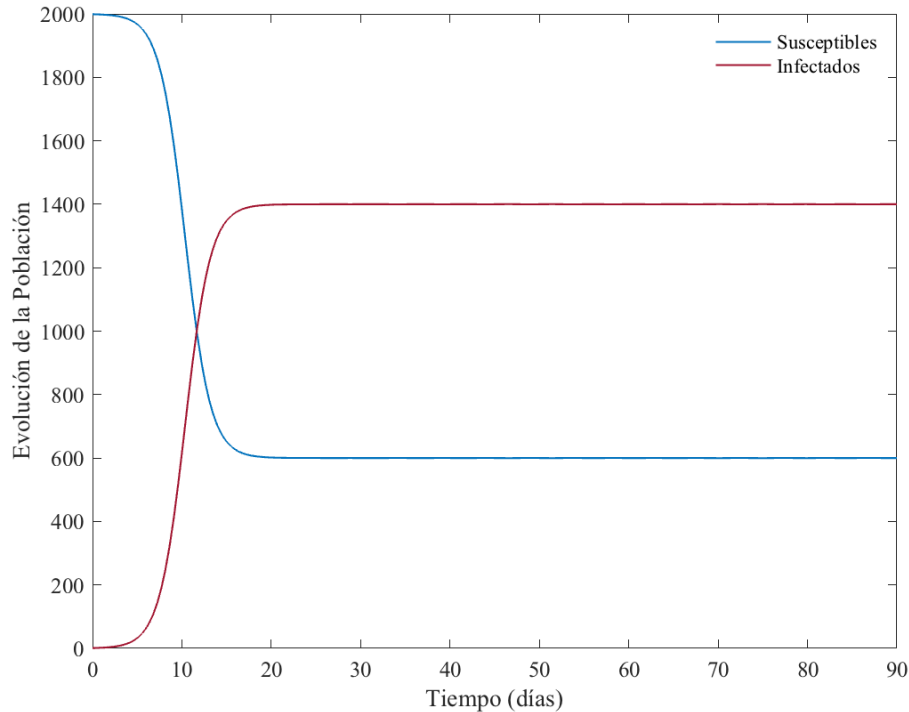
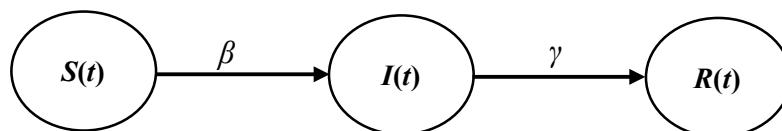


Figura 4.2. Simulación la dinámica de una enfermedad para el modelo SIS con una tasa de infección o contagio $\beta = 5 \cdot 10^{-4}$ y una tasa de recuperación $\gamma = 0.3$, con $S_0=1999$ e $I_0=1$, siendo $\mathcal{R}_0=3.33$.

4.2.2 Modelos de enfermedades que confieren inmunidad tras la infección

Cuando los individuos que superan una enfermedad adquieren inmunidad ante ésta durante un periodo de tiempo prolongado, se estaría ante modelos tipo SIR, SEIR. El modelo básico más ampliamente utilizado es el denominado SIR, y su dinámica de propagación se presenta con los tres estados siguientes.



Según este esquema, los individuos susceptibles que no tienen inmunidad al agente infeccioso pueden infectarse con una tasa de contagio o infección β . Si es así, los individuos que están actualmente infectados pueden transmitir la infección otros individuos susceptibles con los que contacten; y finalmente los individuos infectados se recuperaran con una tasa γ , tras d días de padecer la infección, siendo ahora inmunes a ésta, y no contagiando a otros individuos. El modelo, puede formularse para una población de N individuos con el siguiente sistema de ecuaciones diferenciales ordinarias, con $N = S + I + R$ y $\mathcal{R}_0 = \beta N/\gamma$.

$$\frac{dS(t)}{dt} = -\beta SI, \quad S(0) > 0 \quad 4.5$$

$$\frac{dI(t)}{dt} = \beta SI - \gamma I, \quad I(0) > 0 \quad 4.6$$

$$\frac{dR(t)}{dt} = \gamma I, \quad R(0) = 0 \quad 4.7$$

La Figura 4.3 representa una simulación del modelo SIR. Este modelo se aplica a enfermedades víricas de corto periodo de incubación, tales como la gripe común, y más recientemente para obtener modelos básicos de la COVID-19.

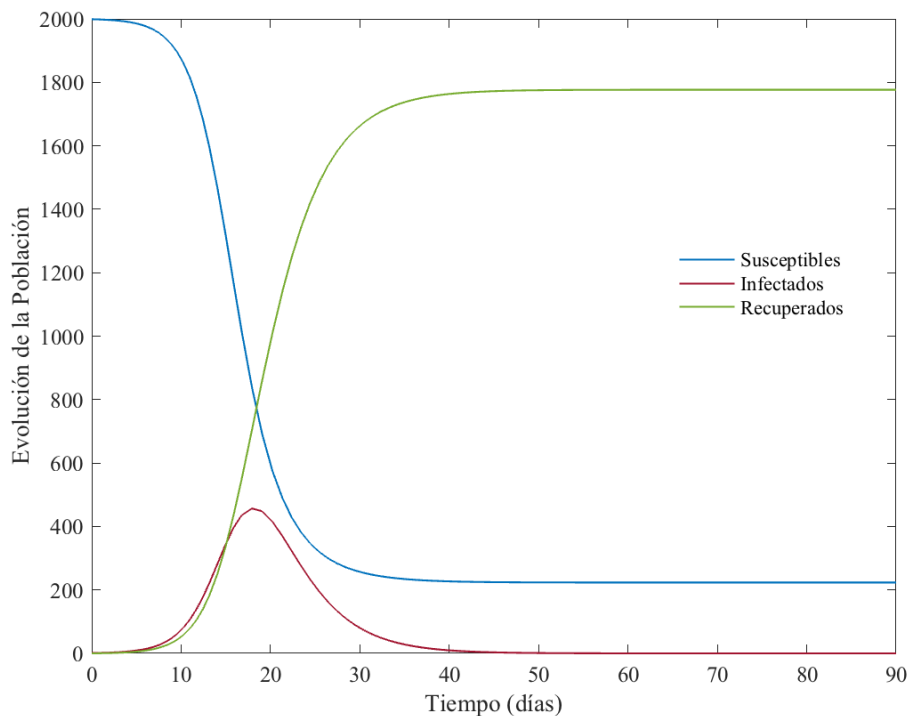
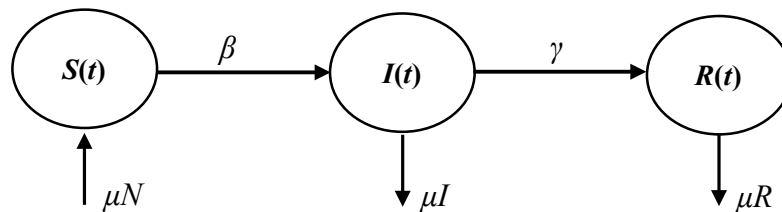


Figura 4.3. Simulación de la dinámica de una enfermedad para el modelo SIR con una tasa de infección o contagio $\beta = 3,7 \cdot 10^{-4}$ y una tasa de recuperación $\gamma = 0.3$, con $S_0 = 1999$ e $I_0 = 1$, siendo $\mathcal{R}_0 = 2.46$.

En otros casos, la dinámica de la enfermedad se desarrolla en un periodo de tiempo suficientemente extenso como para que deban tenerse en cuenta aspectos demográficos como los nacimientos y muertes. En este caso, el modelo es adaptado para esta circunstancia y se incluye una tasa de nacimientos en los individuos susceptibles, proporcional al tamaño total de la población y, a la vez se contemplaba una tasa de mortalidad en cada uno de los estados (infectados y recuperados) proporcional al número de individuos en dicho estado. Este modelo permite que el tamaño total de la población crezca o desaparezca exponencialmente, si las tasas de natalidad y mortalidad son desiguales. En el modelo SIR con nacimientos y muertes, la dinámica de propagación se representa con los siguientes tres estados, siendo β , y γ las tasas de contagio y recuperación, y μ la tasa de natalidad de N nuevos susceptibles y mortalidad en infectados y recuperados [122].



En este caso, la dinámica del modelo se rige por el siguiente sistema de ecuaciones diferenciales ordinarias [122].

$$\frac{dS(t)}{dt} = -\beta SI + \mu(N - S), \quad S(0) > 0, \quad N > 0 \quad 4.8$$

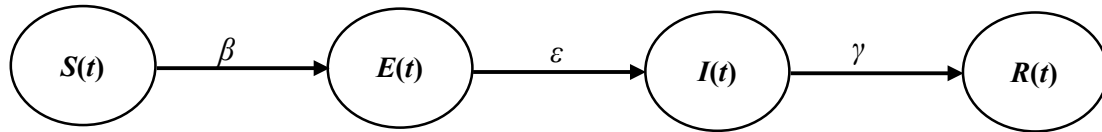
$$\frac{dI(t)}{dt} = \beta SI - \gamma I - \mu I, \quad I(0) > 0 \quad 4.9$$

$$\frac{dR(t)}{dt} = \gamma I - \mu R, \quad R(0) = 0 \quad 4.10$$

La inclusión de las tasas de nacimientos y fallecimiento por causas naturales en la población, puede aplicarse a cualquier modelo epidemiológico, siempre que, como ya se ha comentado, la enfermedad se mantenga en la población en un periodo o si se desea obtener una mayor precisión en los resultados del modelo. El número reproductivo básico viene dado por $\mathcal{R}_0 = \beta N / (\gamma + \mu)$ [122].

En ciertos modelos básicos, se tiene en cuenta un estado intermedio entre el susceptible y el infectado, en el que el individuo está expuesto a la enfermedad. Por ejemplo, en el modelo SEIR, se incorpora el grupo expuesto con un período medio de

exposición o incubación de la enfermedad de $1/\epsilon$. Su dinámica de propagación se presenta, por tanto, con los siguientes cuatro estados.



El modelo, puede formularse para una población de N individuos con siguiente sistema de ecuaciones diferenciales ordinarias, con $N = S + E + I + R$, y $\mathcal{R}_0 = \beta N/\gamma$.

$$\frac{dS(t)}{dt} = -\beta SI, \quad S(0) > 0 \quad 4.11$$

$$\frac{dE(t)}{dt} = \beta SI - \epsilon E, \quad E(0) = 0 \quad 4.12$$

$$\frac{dI(t)}{dt} = \epsilon E - \gamma I, \quad I(0) > 0 \quad 4.13$$

$$\frac{dR(t)}{dt} = -\gamma I, \quad R(0) = 0 \quad 4.14$$

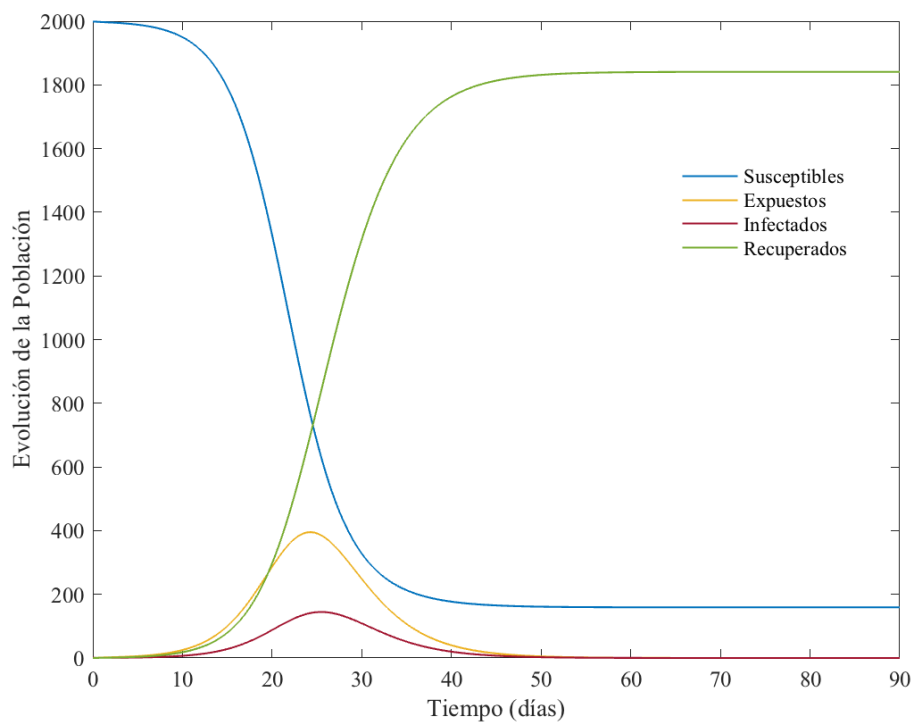


Figura 4.4. Simulación de la dinámica de una enfermedad para el modelo SEIR. Tomando como parámetros $\beta = 1 \cdot 10^{-3}$, $\epsilon = 0.3$, $\gamma = 0.8$, $S_0 = 1999$, $E_0 = 0$, e $I_0 = 1$, siendo $\mathcal{R}_0 = 2.50$.

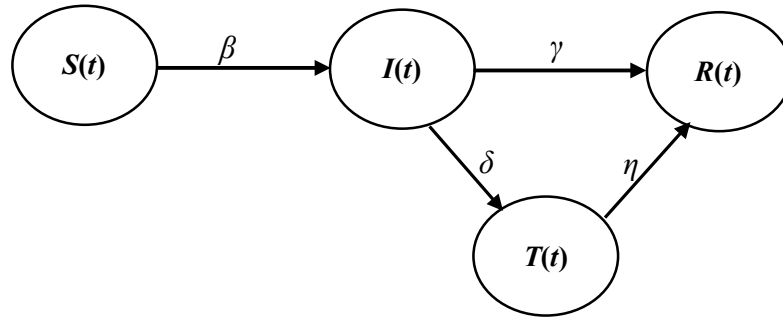
La Figura 4.4 representa una simulación del modelo SEIR. Este modelo se aplica a enfermedades víricas con altos periodos de incubación tales como la varicela, la rubeola, las paperas o la viruela, y como otro modelo básico para el estudio del SARS o de la COVID-19. Si bien en este último caso, los datos de los contagios y las sucesivas olas han demostrado que un modelo más adecuado para estudiar su dinámica de propagación debería contemplar nuevamente a los susceptibles, convirtiéndose en un modelo SEIRS.

4.3 Extensión de los modelos epidemiológicos básicos

Los modelos simples presentados anteriormente están diseñados para resaltar el comportamiento cualitativo de una enfermedad de modo general. Sin embargo, estos modelos tienen un valor adicional ya que como veremos a continuación, son la base para el desarrollo de modelos que incluyen una estructura más detallada. Partiendo de los modelos básicos anteriores, se han desarrollado modelos más complejos que incluyen otros tipos de compartimentos o grupos de individuos. Por ejemplo, los modelos en los que se contempla algún tipo de tratamiento preventivo, tal como la vacunación refleja, la forma de abordar algunas enfermedades, como la gripe común, el sarampión o la rubeola, protegiendo a los individuos contra la infección antes del comienzo de una epidemia. También existen tratamientos en los que se protege al individuo cuando ya ha sido infectado, reduciendo en este caso el tiempo de recuperación de la enfermedad. En otros casos, la enfermedad no se transmite directamente entre personas, si no que existe un vector de contagio intermedio, como en el caso de la Malaria que se transmite por la picadura de un mosquito. Por último, hay situaciones en las que no se dispone de vacuna o tratamiento específico contra una determinada enfermedad, tal como ocurrió con el brote epidémico del SARS-CoV en los años 2002 y 2003, y sin lugar a dudas, tal y como ha ocurrido recientemente con el COVID-19. En estos casos, la única actuación posible para detener la propagación de la enfermedad es la aplicación de políticas de confinamiento y control tales como la cuarentena de los expuestos asintomáticos, o el aislamiento de la población de expuestos e infectados en la fase temprana de la enfermedad, incluso el confinamiento del conjunto de la población de susceptibles.

4.3.1 Modelos epidemiológicos que contemplan tratamientos de la enfermedad

En primer lugar, tomando como referencia el caso de individuos tratados cuando adquieren la enfermedad, el modelo se compondría de los compartimentos o grupos de individuos Susceptibles, Infectados, Tratados y Recuperados, siendo su dinámica de propagación representada por los siguientes cuatro estados.



La interpretación de este diagrama sería la siguiente. Una vez definida la tasa de contagio β , y una tasa de recuperación α , se supone que hay un tratamiento para la infección y que éste reduce el tiempo de recuperación del individuo. En tal caso, se asume una fracción γ por unidad de tiempo de individuos infectados para el tratamiento, y ese tratamiento reduce la infectividad en una fracción δ , siendo η la tasa de recuperación de la clase tratada. Su dinámica queda definida por el siguiente sistema de ecuaciones diferenciales ordinarias para $N = S + I + T + R$ [104].

$$\frac{dS(t)}{dt} = -\beta S[I + \delta T], \quad S(0) > 0 \quad 4.15$$

$$\frac{dI(t)}{dt} = \beta S[I + \delta T] - (\alpha + \gamma)I, \quad I(0) > 0 \quad 4.16$$

$$\frac{dT(t)}{dt} = \gamma I - \eta T, \quad T(0) > 0 \quad 4.17$$

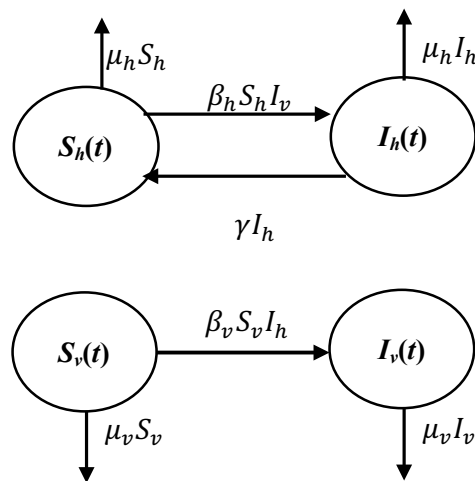
$$\frac{dR(t)}{dt} = \alpha I + \eta T, \quad R(0) = 0 \quad 4.18$$

siendo el número reproductivo básico de este modelo [104].

$$\mathcal{R}_0 = \frac{\beta N}{\alpha + \gamma} + \frac{\gamma}{\alpha + \gamma} \frac{\beta \delta N}{\eta}$$

4.3.2 Modelos epidemiológicos que contemplan vectores de contagio

En ciertos modelos se tiene en cuenta que la transmisión de la enfermedad no se realiza directamente de persona a persona, si no a través de un vector de contagio. En este grupo se encuentran enfermedades transmitidas por mosquitos, como pueden ser la Malaria, el Dengue, o la fiebre del Nilo entre otras. La dinámica de paso de la población de un compartimento a otro es ahora gobernada no sólo por la dinámica de la propia población de susceptibles e infectados, sino también por la dinámica de la población del vector de contagio. Como ejemplo, en el esquema adjunto se presenta un modelo simplificado para la dinámica de propagación de este tipo de enfermedades, el cual se compone de dos modelos epidémicos básicos acoplados, del tipo que no confieren inmunidad al individuo infectado, un modelo SIS y un modelo SI en los que se tienen en cuenta las tasas de natalidad y mortalidad naturales.



La interpretación de este diagrama sería la siguiente. Asumiendo que los vectores de contagio permanecen infectados durante toda su vida, los huéspedes susceptibles S_h se convierten en huéspedes infecciosos I_h a un ritmo de contagio $\beta_h S_h I_v$, causado por el contacto con los vectores de infección I_v . Por otra parte, los vectores de contagio susceptibles S_v se convierten en vectores infecciosos I_v a un ritmo de contagio $\beta_v S_v I_h$, causado por el contacto con huéspedes infectados. El resto de parámetros representan las tasas de mortalidad para huéspedes y vectores de contagio, μ_h y μ_v ; y las tasas de nuevos susceptibles en ambas poblaciones Π_h y Π_v , siendo γ la tasa de recuperación de los huéspedes infectados. Con estos parámetros, la dinámica del modelo se define por el siguiente sistema de ecuaciones diferenciales ordinarias [122].

$$\frac{dS_h(t)}{dt} = \Pi_h - \mu_h S_h - \beta_h S_h I_v + \gamma I_h \quad 4.19$$

$$\frac{dI_h(t)}{dt} = \beta_h S_h I_v - (\gamma + \mu_h) I_h \quad 4.20$$

$$\frac{dS_v(t)}{dt} = \Pi_v - \mu_v S_v - \beta_v S_v I_h \quad 4.21$$

$$\frac{dI_v(t)}{dt} = \beta_v S_v I_h - \mu_v I_v \quad 4.22$$

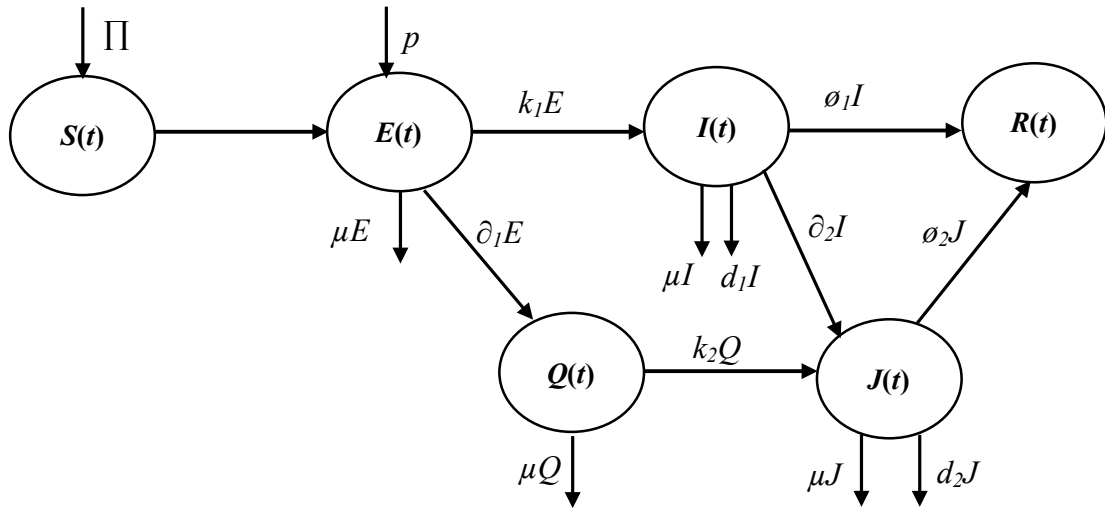
Obteniéndose un valor para el número reproductivo básico dado por la siguiente expresión, siendo $S_{h0} = \Pi_h/\mu_h$ y $S_{v0} = \Pi_v/\mu_v$ [122]

$$\mathcal{R}_0 = \sqrt{\frac{\beta_h \beta_v S_{h0} S_{v0}}{(\gamma + \mu_h) \mu_v}}$$

4.3.3 Modelos epidemiológicos que contemplan políticas de confinamiento

Hasta la aparición de la epidemia del coronavirus SARS-CoV entre 2002 y 2003, los modelos epidemiológicos que contemplaban estados como la cuarentena y el aislamiento prácticamente no habían sido considerados. Uno de los primeros modelos de este tipo fue propuesto por Gumel y otros [108] para modelar la eficacia de las estrategias adoptadas para detener la epidemia la propagación del SARS-CoV zonas como Beijing, Hong Kong o Singapur. Este modelo, contemplaba la posibilidad de que el contagio se produjese no sólo por los individuos infectados, sino también por individuos asintomáticos y por la baja eficiencia de las políticas de cuarentena y aislamiento. Un comportamiento similar al del SARS-CoV, fue observado, pero con mucha más intensidad, en la epidemia global o pandemia del COVID-19, por lo que el modelo de Gumel ha sido tomado como referencia en muchos casos para el estudio del comportamiento del COVID-19. A modo de ejemplo, y para entender la complejidad de este tipo de modelos, en el esquema adjunto [108] se pueden ver los estados que lo componen, pudiéndose identificar, que se parte de un modelo SEIR básico, al que se le añaden los individuos que aunque se han expuesto al virus por el contacto con otros individuos infectados, permanecen asintomáticos y que son puestos en cuarentena (Q);

y los individuos que son aislados u hospitalizados (J) una vez que se les diagnostica la que han contraído la enfermedad.



El flujo de individuos de un estado o compartimento a otro, así como su dinámica queda definida para una población $N = S + E + Q + I + J + R$ por el siguiente sistema de seis ecuaciones diferenciales ordinarias [108].

$$\frac{dS}{dt} = \Pi - \frac{\beta S(I_S + k_E E + k_Q I_A + k_J J)}{N} - \mu S \quad 4.23$$

$$\frac{dE}{dt} = p - \frac{\beta S(I_S + k_E E + k_Q I_A + k_J J)}{N} - (\partial_1 + k_1 + \mu)E \quad 4.24$$

$$\frac{dQ}{dt} = \partial_1 E - (k_2 + \mu)Q \quad 4.25$$

$$\frac{dI}{dt} = k_1 E - (\partial_2 + d_1 + \phi_1 + \mu)I \quad 4.26$$

$$\frac{dJ}{dt} = \partial_2 I + k_2 Q - (\phi_2 + d_2 + \mu)J \quad 4.27$$

$$\frac{dR}{dt} = \phi_1 I + \phi_2 J \quad 4.28$$

Al igual que en los modelos anteriores, β representa la tasa de contagio, los parámetros k_1 , k_2 , y ∂_1 , ∂_2 representan las diversas tasas o tiempo medio de permanencia de cada individuo en el compartimento correspondiente, mientras que ϕ_1 , ϕ_2 representan las tasas de recuperación de los individuos infectados y los hospitalizados respectivamente. El parámetro Π es la tasa de nacimientos en la población de susceptibles, p representa la entrada de individuos infectados pero asintomáticos, μ

representa la tasa de mortalidad natural de la población, y d_1 y d_2 , son las tasas de mortalidad para los infectados y hospitalizados respectivamente. Finalmente, el modelo también contempla la posibilidad de transmisión del virus por individuos asintomáticos, y por fallos en la implementación de medidas protectoras o de higiene durante la cuarentena y el aislamiento, incluyendo los parámetros k_E , k_Q y k_J respectivamente para cada caso. El número reproductivo básico \mathcal{R}_0 , dado por la expresión 3.26, y el número reproductivo de control \mathcal{R}_c por la expresión 3.27. El número \mathcal{R}_c se utiliza cuando las medidas de control (cuarentena y aislamiento) han sido puestas en marcha, y si éstas han dado resultado, debe verificarse que $\mathcal{R}_c < \mathcal{R}_0$ [108].

$$\mathcal{R}_0 = \frac{\beta k_E}{(k_1 + \mu)} + \frac{\beta k_1}{(k_1 + \mu)(d_1 + \phi_1 + \mu)} \quad 4.29$$

$$\mathcal{R}_c = \frac{\beta k_E}{\lambda_1} + \frac{\beta k_1}{\lambda_1 \lambda_2} + \frac{k_Q \beta \partial_1}{\lambda_1 \lambda_4} + \frac{k_J \beta k_1 \partial_2}{\lambda_1 \lambda_2 \lambda_3} + \frac{k_J \beta \partial_2 k_1}{\lambda_1 \lambda_3 \lambda_4} \quad 4.30$$

donde

$$\lambda_1 = (\partial_1 + k_1 + \mu), \lambda_2 = (\partial_2 + d_1 + \phi_1 + \mu), \lambda_3 = (\phi_2 + d_2 + \mu), \lambda_4 = (k_2 + \mu)$$

Como se ha visto, los modelos epidemiológicos complejos están formados por modelos simples como los presentados en el apartado anterior. Siguiendo con esta filosofía, se pueden ir añadiendo compartimentos o grupos de población, así como aspectos demográficos (edad, sexo, etc.) con el fin de cubrir las posibles variantes que intervienen en la propagación de una determinada enfermedad.

En la mayoría de las áreas de modelado matemático, como ocurre en el de la transmisión de enfermedades, siempre es preciso buscar el equilibrio entre el uso de modelos simples que, asumiendo una serie de hipótesis, están pensados para resaltar el comportamiento cualitativo general del modelo; y el uso de modelos más complejos, cuyo objetivo es modelar situaciones específicas aportando predicciones cuantitativas a corto plazo. En este sentido, la resolución analítica de los modelos detallados es generalmente difícil, de hecho, se ha demostrado que modelos complejos que se han desarrollado para adaptarse a la dinámica de una determinada enfermedad con el fin de hacerlos más realistas, exhiben comportamientos cualitativos muy similares al observado en modelos epidemiológicos realmente simples. En concreto, el modelo

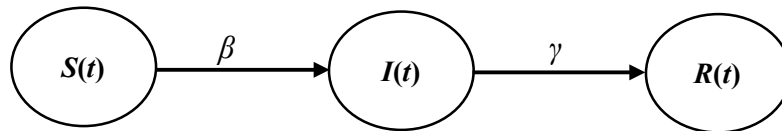
SEIQR expuesto anteriormente, ha demostrado tener un comportamiento asintótico a similar al SIR básico [104]. Para el desarrollo de esta investigación, se ha utilizado como base el modelo epidemiológico SIR, tanto en su formulación determinista como en la estocástica. No obstante, y con la intención de aportar una visión más global de cómo se ha llegado a la elección de este modelo y su aplicación al análisis de la propagación de ataques *jamming*, también se mencionarán en este trabajo los modelos epidemiológicos que se utilizaron en el inicio de la investigación.

4.4 El modelo determinista Susceptible-Infectado-Recuperado

El modelo epidemiológico SIR determinista además de poseer un largo historial de aplicaciones, está considerado un estándar en el estudio de enfermedades. Sin embargo, pese a ser un modelo extremadamente simple, desde el punto de vista matemático resulta complejo obtener una expresión exacta para las soluciones del sistema de ecuaciones diferenciales ordinarias que lo rigen. Como ejemplo, Kermack y McKendrick [103] encontraron una solución aproximada para el número de infectados $I(t)$ para su modelo SIR básico si bien, esta aproximación demostró ser válida solo al inicio de la epidemia, o bien para todo el tiempo de duración de ésta siempre que el valor de \mathcal{R}_0 permaneciese próximo a la unidad.

El interés principal de aplicación del modelo SIR, es el estudio de la dinámica de un brote epidémico único. Consideremos una población N , donde $S(t)$, $I(t)$ y $R(t)$ representan el número de individuos en los grupos o compartimientos Susceptibles, Infectados y Recuperados, respectivamente, en el tiempo t . Se define β como la tasa de infección o tasa de contagio, que representa la probabilidad por cada individuo y por unidad de tiempo de contraer la enfermedad, siendo sus dimensiones habituales en el estudio de brotes epidémicos [$\text{días}^{-1} \cdot \text{número de individuos}$]. Por otra parte, se define γ como el periodo de recuperación de los individuos infectados siendo sus dimensiones [días^{-1}]. Se considera, por tanto, que el periodo de incubación es despreciable, esto es, el tiempo de exposición desde que un individuo es infectado hasta que el individuo empieza a ser infeccioso es cero. Remarcar que la tasa de infección depende de cada enfermedad y de ambas poblaciones, mientras que el periodo de recuperación sólo depende de la población de individuos infectados que haya en cada momento. Además, se asume que el número de individuos de la población N es lo suficientemente grande

como para considerar que la cantidad de individuos de cada grupo $S(t)$, $I(t)$ y $R(t)$ puede representarse por una función continua del tiempo. Por lo tanto, tomando como referencia el esquema de flujo de paso de los individuos de un compartimento a otro, se asumen las siguientes tres hipótesis:



1ª Hipótesis: Esta hipótesis se basa en la Ley de Acción de Masas y asume que un individuo infectado de la población puede transmitir la infección mediante βN contactos por unidad de tiempo con otros miembros, donde N es el tamaño de la población. Dado que la probabilidad de que un contacto aleatorio de un infectado I sea con un susceptible S –que luego puede transmitir la infección– el número de nuevas infecciones es $(\beta N) \cdot (S/N)$, lo que da una tasa de nuevas infecciones $(\beta N) \cdot (S/N)I = \beta SI$ [104].

2ª Hipótesis: Esta hipótesis determina que los miembros infectados de la población abandonan su grupo o compartimento a una velocidad $\gamma \cdot I$. Si bien asumir que la tasa de recuperación es proporcional al número de infecciones no tiene un claro significado epidemiológico, se puede demostrar que la fracción de individuos infectados que permanecen en ese estado después de haber sido infectados es $e^{-\gamma s}$, con s unidades de tiempo. De este modo se puede determinar que la duración del período infeccioso se distribuye exponencialmente con media $\int_0^{\infty} e^{-\gamma s} ds = 1/\gamma$ [104]. A partir de esta suposición, la dinámica del grupo Infectado queda definido como $\beta SI - \gamma \cdot I$, y la dinámica del grupo Recuperado será, por tanto, $\gamma \cdot I$.

3ª Hipótesis: Esta última hipótesis considera que el número de individuos N en la población es constante, esto es, se considera una población “cerrada” que no recibe nuevos individuos ni existen individuos que abandonan la población, cumpliéndose que $N(t) = S(t) + I(t) + R(t)$. Esto aplica cuando la escala de tiempo de propagación de la enfermedad es más rápida que la escala de tiempo de nacimientos y muertes, por lo tanto, los efectos demográficos pueden ignorarse y el tamaño de la población es constante en cualquier instante t [104].

Según estas hipótesis, la expresión matemática del modelo se puede escribir mediante el siguiente sistema de ecuaciones diferenciales ordinarias que ya se vio con anterioridad:

$$\frac{dS(t)}{dt} = -\beta SI, \quad S(0) > 0 \quad 4.5$$

$$\frac{dI(t)}{dt} = \beta SI - \gamma I, \quad I(0) > 0 \quad 4.6$$

$$\frac{dR(t)}{dt} = -\gamma I, \quad R(0) = 0 \quad 4.7$$

Hay que señalar, que al formular estos modelos utilizando ecuaciones diferenciales, se asume que el proceso epidémico es determinista, y que el comportamiento de la población estará completamente determinado por las condiciones iniciales y por las reglas establecidas en el modelo. Además, el sistema se considera autónomo e invariante ya que tanto la tasa de infección β como la tasa de recuperación γ no cambian con el tiempo. Como ya se comentó con anterioridad, el primero de estos parámetros, depende de cada enfermedad, mientras que el segundo solo depende de las características fisiológicas y demográficas de población de individuos infectados que tienen en cada instante.

Antes de abordar el estudio matemático en profundidad del modelo SIR, se puede realizar primer un análisis desde el punto de vista cualitativo, el cual proporcionará importantes propiedades sobre el comportamiento de las variables que lo integran.

Para comenzar, con este análisis cualitativo, tomemos como referencia las ecuaciones 4.5 y 4.6 del modelo, teniendo en cuenta que la resolución del sistema sólo puede tener sentido siempre y cuando el número de individuos de cada grupo $S(t)$, $I(t)$ y $R(t)$, permanezcan en valores positivos.

De la ecuación 4.5 se extrae que $dS/dt < 0$ para todo t , mientras que agrupando los términos de la ecuación 4.6 y tomando $I(\beta S - \gamma) > 0$, se obtiene que $dI/dt > 0$ si y solo si $S > \gamma/\beta$. De estas desigualdades se deduce que los individuos infectados aumentarán en la población siempre que la proporción de susceptibles sea mayor que la relación γ/β , pero a su vez, y dado que el número de susceptibles es decreciente durante todo el tiempo que dure la enfermedad, el número de infectados disminuirá paulatinamente hasta que finalmente se acerque a cero. Por lo tanto, si el número de susceptibles en la población inicial S_0 es menor que γ/β , el número de infectados disminuirá directamente

hasta cero y la enfermedad se extinguirá por si sola en la población (*Disease-free Equilibrium*, DFE). Por el contrario, si se cumple que el número de susceptibles en la población inicial S_0 es mayor que γ/β , podría producirse un brote epidémico. Este proceso se inicia con un aumento de los infectados hasta alcanzar el número máximo cuando $S = \gamma/\beta$, para posteriormente ir disminuyendo hasta aproximarse a cero, a la vez que aumenta el número de recuperados. En el estado de equilibrio endémico (*Endemic Equilibrium*, EE), la enfermedad permanecerá durante un tiempo más o menos prolongado entre la población hasta que desaparece. Sin embargo, si se produce una aportación continuada de individuos susceptibles en la población, la enfermedad podría mantenerse en ésta de forma permanente, convirtiéndose en una enfermedad endémica.

Este primer análisis cualitativo, permite vislumbrar la existencia de un valor umbral γ/β que determinará si el número de infectados disminuirá directamente hasta cero y la enfermedad se extinguirá por si sola en la población o si, por el contrario, la enfermedad permanecerá durante un tiempo entre la población convirtiéndose en una epidemia hasta alcanzar el número máximo de infectados. Como ya se adelantó, Kermack-McKendrick postularon en su *teorema del umbral* [103], que la introducción de individuos infectados en una población no provocará un brote epidémico salvo que la densidad de la población susceptible supere un cierto valor crítico. La cantidad $\beta S_0/\gamma$ corresponde con el valor crítico o umbral de la epidemia. Éste será, el denominado *Número Reproductivo Básico* \mathcal{R}_0 , y representa el número promedio de infecciones secundarias generadas por el primer individuo infectado o “*paciente cero*” que se introduce en una población de individuos completamente susceptibles.

Por otra parte, desde un punto de vista matemático, al tratarse de un sistema de ecuaciones diferenciales ordinarias no lineales, la solución analítica a este sistema es muy complicada de obtener, aunque se pueden encontrar diversas aproximaciones, [103], [104], [122], [123], [124] entre otras. Como ejemplo, Harko, Lobo y Mak [124] propusieron un modo para obtener la solución analítica exacta del modelo SIR, con y sin dinámica de nacimientos y fallecimientos para una población constante. Las soluciones, obtenidas en forma paramétrica, correspondiendo en el modelo SIR básico a un sistema equivalente con $x = S$, $y = I$, y $z = R$ y $N = N_1 + N_2 + N_3$, siendo ésta la población total constante.

$$\frac{dx}{dt} = -\beta xy, \quad x(0) = N_1 \quad 4.31$$

$$\frac{dy}{dt} = \beta xy - \gamma y, \quad y(0) = N_2 \quad 4.32$$

$$\frac{dz}{dt} = -\gamma z, \quad z(0) = N_3 \quad 4.33$$

Las soluciones a este sistema, vienen dadas en forma paramétrica por

$$x = x_0 u$$

$$y = \frac{\gamma}{\beta} \ln u - x_0 u - \frac{C_1}{\beta}$$

$$z = -\frac{\gamma}{\beta} \ln u$$

con $u = e^{-\frac{\beta}{\gamma} z}$, con $u(0) = e^{-\frac{\beta}{\gamma} N_3}$, y $x_0 = e^{-\frac{\beta}{\gamma} z_0}$.

Sumando las tres ecuaciones se obtiene que $x + y + z = C_1/\beta$, de donde se deduce que $C_1 = -\beta N$, obteniendo así que $x + y + z = N$.

Un enfoque matemático típico para el estudio de la dinámica de propagación un brote epidémico, consiste analizar la estabilidad local de los puntos de equilibrio del sistema de ecuaciones diferenciales que lo componen. La propiedad principal de estos puntos es que, si se produce una ligera perturbación en el sistema, y éste se desplaza a algún punto cercano al punto estacionario, entonces el sistema debería volver a este punto estacionario [125]. Para el caso del modelo SIR, estos puntos vienen dados por las soluciones obtenidas al igualar a cero de las ecuaciones 4.5 y 4.6, con lo que se establece que el flujo de individuos entre compartimentos es constante.

$$\frac{dS(t)}{dt} = -\beta SI = 0 \quad 4.5$$

$$\frac{dI(t)}{dt} = \beta SI - \gamma I = I(\beta S - \gamma) = 0 \quad 4.6$$

Como ya se comentó anteriormente, desde el punto de vista epidemiológico, los puntos de equilibrio de interés son el libre de enfermedad (DFE) y el endémico (EE). Las soluciones a este sistema vienen dadas por los valores $I = 0$, y $\beta S - \gamma = 0$, con $I > 0$. Es fácil de comprobar que con $I = 0$, la infección no ha progresado entre la población, por lo que estaríamos ante el punto del DFE, cuyo equilibrio viene dado por $(N, 0, 0)$. Por el contrario, el Equilibrio Endémico corresponde al estado en el que los individuos

infectados persisten indefinidamente entre la población, con lo que $I > 0$. Desde el punto de vista epidemiológico, este equilibrio requiere una aportación continua de individuos susceptibles dentro de la población, ya sea por nacimientos o por pérdida de inmunidad ante la infección. Para el caso del modelo SIR sin demografía, el número de infectados siempre vuelve a cero una vez que el brote epidémico ha finalizado y se alcanza el estado estacionario del sistema, obteniendo un equilibrio de la forma $(S_\infty, 0, R_\infty)$, donde $N = N_\infty = S_\infty + R_\infty$.

Para analizar la estabilidad local de estos puntos, se pueden emplear varias técnicas, incluyendo, entre otras, las que hacen uso del operador denominado de *Próxima Generación* (*Next-Generatiom Operator*) sugerido por Diekmann, Heesterbeek, y Metz [114], funciones de *Poincaré-Lyapunov*, o aplicar técnicas de linealización mediante operadores *Jacobianos* [125]. En el Apéndice I, se ha incluido el desarrollo matemático del operador denominado de *Próxima Generación*, mientras que, en este apartado, se expone el método de operadores *Jacobianos*. Con este operador, se trata de demostrar que, si el sistema dinámico es hiperbólico en un punto de equilibrio, entonces ese punto es asintóticamente estable si su linealización es asintóticamente estable. Además, si un punto de equilibrio es asintóticamente estable, todos los valores propios del polinomio característico asociado a la matriz *Jacobiana* han de tener partes reales negativas, lo que se cumple si y solo si $\det(J) > 0$ y $\text{tr}(J) < 0$ [125]. Se puede demostrar [126] que la linealización del sistema anterior alrededor de cada equilibrio utilizando la matriz *Jacobiana* evaluada en el DFE, indica que para que todos los valores propios tengan partes reales negativas ha de verificarse que $\beta N/\gamma < 1$; de lo contrario, el punto de equilibrio es localmente inestable. En este último caso, el punto crítico del sistema $(S_\infty, 0, R_\infty)$ viene dado por $(\gamma N/\beta, 0, 1 - \gamma N/\beta)$. Esta solución está en concordancia con lo que ya se indicó en el análisis cualitativo anterior, dónde se vio que cuando el número de susceptibles en la población inicial S_0 es menor que γ/β , entonces el número de infectados disminuirá hasta cero, $I_\infty = 0$ y la enfermedad se extinguirá por si sola en la población. Por el contrario, si el número de susceptibles en la población inicial S_0 es mayor que γ/β , $I(t)$ es creciente y alcanza un único punto crítico no nulo, por lo que se producirá un aumento de los infectados con lo que la enfermedad permanecerá durante un tiempo entre la población y si no hay aporte de susceptibles, el número de infectados disminuirá hasta cero, $I_\infty = 0$.

Para una población N lo suficientemente grande, y tomando como referencia al primer individuo infectado dentro de la población a estudio, esto es $I_0 = 1$, se tendrá que al inicio de la enfermedad (para $t = 0$), $R_0 = 0$ y $S_0 = N - I_0$, con $I_0 \ll N$ por lo que se puede asumir que $S_0 \approx N$, pudiendo asumir por tanto que $\mathcal{R}_0 = \beta N/\gamma$, y el punto crítico $(S_\infty, 0, R_\infty)$ puede escribirse con respecto a \mathcal{R}_0 de la forma $(1/\mathcal{R}_0, 0, 1-1/\mathcal{R}_0)$.

A parte del análisis cualitativo de las ecuaciones anteriores, también pueden obtenerse ciertas soluciones de interés si en lugar de resolver el sistema en función del tiempo, se realizan algunas operaciones algebraicas sobre estas ecuaciones [121]. Por ejemplo, dividiendo las ecuaciones 4.5 y 4.6 obtenemos la función

$$\frac{\frac{dS(t)}{dt}}{\frac{dR(t)}{dt}} = \frac{-\beta SI}{\gamma I} = \frac{-\beta S}{\gamma} = \frac{dS(t)}{dR(t)} = -R_0 S \rightarrow \int_0^t dR = \int_0^t \frac{-1}{R_0 S} dS \quad 4.34$$

Integrando con respecto a R , y tomando $R_0 = 0$, se obtiene como solución que

$$S(t) = S_0 e^{-R_0 R(t)} \quad 4.35$$

Partiendo de esta solución, también podemos deducir que la proporción de individuos recuperados cuando $t \rightarrow \infty$, obedecerá a la ecuación trascendental

$$R_{t \rightarrow \infty} = N - S_0 e^{-R_0 [R_\infty - R_0]} \quad 4.36$$

De esta ecuación se extrae que al final de una epidemia, siempre que $S_0 > 0$, no todos los individuos de la población se habrán recuperado, y dado que $I_\infty = 0$, se deduce que siempre quedará una fracción de la población susceptibles que no se verá infectada.

Por otro lado, dividiendo las ecuaciones 4.5 y 4.6 obtenemos

$$\frac{\frac{dI(t)}{dt}}{\frac{dS(t)}{dt}} = \frac{\beta SI - \gamma I}{-\beta SI} = \frac{dI(t)}{dS(t)} = -1 + \frac{\gamma}{\beta S} \rightarrow \int_0^t dI = - \int_0^t dS + \int_0^t \frac{\gamma}{\beta S} dS \quad 4.37$$

Integrando con respecto a I , se obtiene que

$$I = -S + \frac{\gamma}{\beta} \ln S + c \quad 4.38$$

Proporcionando las curvas de las soluciones (S, I) del sistema u órbitas en el plano de fases siendo c una constante que se determina con los valores iniciales S_0, I_0 . Estas órbitas de las curvas en el plano de fases, representan el movimiento de las soluciones $S(t), I(t)$ [125]. Una forma alternativa de representar estas órbitas, es mediante la función 4.39.

$$F(S, I) = S + I - \frac{\gamma}{\beta} \ln S, \quad \text{con } c = S(0) + I(0) - \frac{\gamma}{\beta} \ln S(0) \quad 4.39$$

En la Figura 4.5 se ha representado el plano de fases con las órbitas correspondientes al modelo SIR para las condiciones iniciales $S_0 = 1999$ e $I_0 = 1$, una tasa de recuperación constante $\gamma = 0.3$ y una tasa de infección β variable, obteniendo diferentes valores para el número reproductivo básico \mathcal{R}_0 .

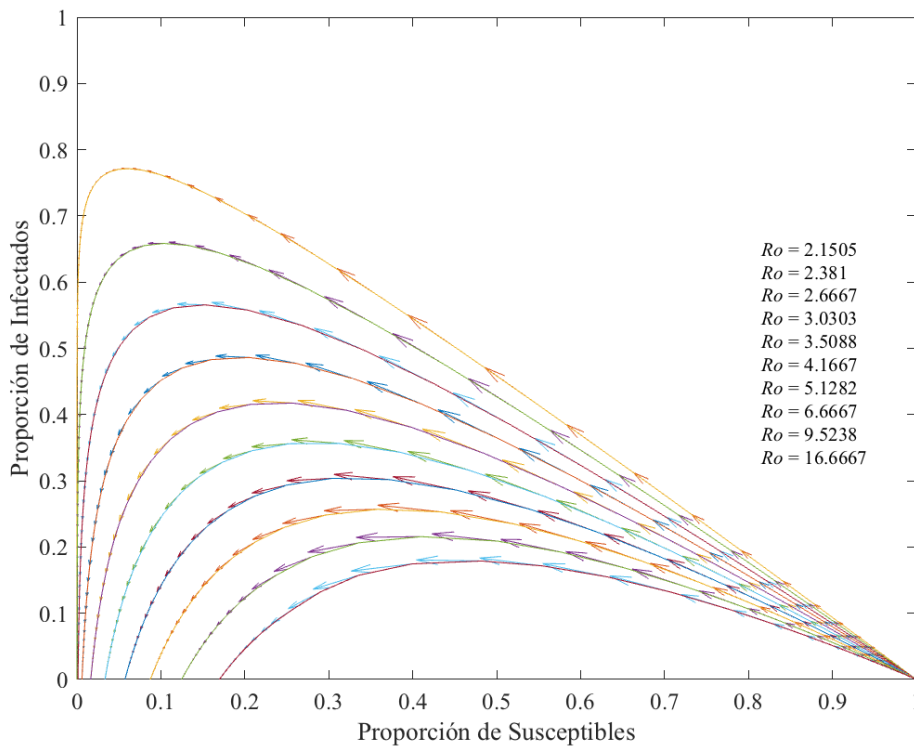


Figura 4.5. Representación de las órbitas del plano de fases para el modelo SIR con condiciones iniciales $S_0 = 1999$ e $I_0 = 1$, $\gamma = 0.3$ y β variable, obteniendo diferentes valores para \mathcal{R}_0 .

Se puede observar que el valor máximo del número de infectados para cada una de las órbitas se obtiene cuando la población de susceptibles alcanza el valor $S(t) = \gamma/\beta$. Así mismo, se observa que ninguna de estas órbitas cruza el eje de Infectados, por lo que $S(t) > 0$ durante todo el tiempo que dure el proceso de la enfermedad. Por lo tanto, se deduce, además que $S_\infty = \lim_{t \rightarrow \infty} S(t) > 0$, lo que implica que parte de la población escapará a la infección. Teniendo estas consideraciones en cuenta, se puede obtener una aproximación de la relación β/γ en función los valores de S_0 y S_∞ [104]. Para ello, se supone que, en una población de susceptibles N suficientemente grande, se introduce un

número pequeño de infectados, siendo $S_0 \approx N$, $I_0 \approx 0$, y $\mathcal{R}_0 = \beta N/\gamma$. Si tenemos en cuenta que $\lim_{t \rightarrow \infty} I(t) = 0$, y que $S_\infty = \lim_{t \rightarrow \infty} S(t)$, entonces de la relación $F(S_0, I_0) = F(S_\infty, 0)$ se tiene que

$$N - \frac{\gamma}{\beta} \ln S_0 = S_\infty - \frac{\gamma}{\beta} \ln S_\infty \quad 4.40$$

de dónde podemos obtener la siguiente relación de β/γ en función de S_0 y S_∞ .

$$\frac{\beta}{\gamma} = \frac{\ln S_0 - \ln S_\infty}{N - S_\infty} \quad 4.41$$

o bien reescrita en términos del número reproductivo básico \mathcal{R}_0 , obtenemos la relación

$$\mathcal{R}_0 = \frac{\ln S_0 - \ln S_\infty}{1 - S_\infty/N} \quad 4.42$$

Si bien hay que destacar que esta estimación sólo podrá obtenerse una vez finalizada la epidemia.

Por último, con base en estas definiciones, se puede obtener un parámetro de gran interés que aportará información relevante sobre la dinámica de la enfermedad, éste es el número máximo de infectados. Este valor se deduce haciendo cero la derivada de $I(t)$ es cero, lo que se cumple cuando $S = \gamma/\beta$. sustituyendo este valor en la Ecuación 4.38 y tomando $I = I_{\max}$, se obtiene que

$$I_{\max} = S_0 + I_0 - \frac{\gamma}{\beta} \ln S_0 - \frac{\gamma}{\beta} + \frac{\gamma}{\beta} \ln \frac{\gamma}{\beta} \quad 4.43$$

Este valor resulta especialmente útil para determinar los efectos de la epidemia al final del período infeccioso.

4.5 Introducción a los modelos epidémicos fenomenológicos

Los modelos epidémicos expuestos hasta ahora en este Capítulo, se basan en enfoques mecánicos o físicos para identificar patrones en los datos observados, que permitan comprender las leyes involucradas en la dinámica de la población o la dinámica de transmisión de una enfermedad. Estos modelos derivan de los modelos matemáticos *compartimentales* propuestos por Kermack y McKendrick [103] o Anderson y May [107], y en ellos se asume que, en ausencia de estrategias de control, la dinámica de crecimiento en la primera etapa de una epidemia (*early epidemic*) es exponencial. Por el contrario, existe una alternativa a estos modelos, en la que se aplica un enfoque empírico sin tener una base específica sobre las leyes físicas o los mecanismos que dan lugar a los patrones observados en los datos. Estos son los denominados modelos fenomenológicos epidémicos. La mayoría de estos modelos, se basan en la Teoría del Crecimiento de la Poblacional [127], [128] y se conocen como Modelos Epidémicos Fenomenológicos, siendo comúnmente utilizados para realizar predicciones a medio plazo de la dinámica de propagación de una enfermedad.

La ecuación que define estos modelos se conoce como Modelo de Crecimiento Genérico y se desarrolla en base tres postulados. El primero afirma que la tasa de crecimiento es conjuntamente proporcional a una función monótona de la distancia generalizada desde el origen al tamaño actual denominado *capacidad reproductiva*, y a una función monótona de la distancia generalizada desde el tamaño actual de la población hasta el tamaño final, denominada *factor limitante* [127], [129]. El segundo postulado restringe la función monótona a la función de *acción de masas*. El tercer postulado aplica restricciones al modelo de tal modo que el número de parámetros a utilizar sea manejable desde el punto de vista matemático.

Con estos postulados de forma convenientemente desarrollados, Turner, Bradley, Kirk y Pruitt, propusieron la siguiente *Ecuación Fundamental de Crecimiento* [127], [129]:

$$\frac{dx}{dt} = \dot{x} = \frac{r}{k^n} x^{1-np} (k^n - x^n)^{1+p} \quad 4.44$$

Donde x es el tamaño del organismo o de la población en el instante t ; r es un valor positivo que denota la tasa de crecimiento intrínseca ($1/t$); k representa tamaño máximo de dicho organismo o población, cuando t aumenta sin límite; y n, p , son parámetros que modelan la curva de crecimiento, cumpliéndose que $n > 0$, y $-1 < p < 1/n$.

La solución a esta ecuación viene dada por la siguiente función obtenida mediante separación de variables [127], [129]:

$$x = \frac{k}{\{1 + [1 + rnp(t - \tau)]^{1/p}\}^{1/n}} \quad 4.45$$

Donde τ es una constante de integración.

Partiendo de esta ecuación y eligiendo de forma adecuada los parámetros k, r, p, n se obtiene una amplia familia de funciones de crecimiento.

4.5.1 Modelos epidémicos de crecimiento exponencial y sub-exponencial

El Modelo de Crecimiento Generalizado (*Generalized Growth Model*, GGM) es un caso especial de aplicación de la ecuación fundamental de tasa de crecimiento, en el que se emplean tan solo dos parámetros, uno de ellos determina la tasa de crecimiento y el otro relaja el supuesto de crecimiento exponencial. El modelo enfatiza la reproducibilidad de las observaciones empíricas y se ha demostrado que es muy útil para modelar epidemias de diversas enfermedades en sus fases tempranas como el SARS, Ébola, Zika o COVID-19 [118], [130], [131], [132], [133]. Este modelo asume una dinámica de crecimiento sub-exponencial al comienzo de la enfermedad en lugar de exponencial y se define mediante la ecuación diferencial 3.56 [131]:

$$\frac{dC(t)}{dt} = C'(t) = rC^p(t) \quad 4.46$$

donde $C'(t)$ representa la incidencia en el tiempo t , mientras que la solución $C(t)$ es el número acumulado de casos en el tiempo t . El parámetro r es un valor positivo que denota la tasa de crecimiento intrínseca ($1/t$), y el parámetro p se considera la *desaceleración del factor de crecimiento* donde $p \in [0, 1]$. La solución a esta ecuación diferencial viene dada por la siguiente fórmula:

$$C(t) = \left(\frac{r}{n}t + A\right) \quad 4.47$$

donde, n es un número entero positivo, y el parámetro de desaceleración del crecimiento viene dado por $p = 1 - 1/n$. A es una constante que depende de las condiciones iniciales y se define como $A = \sqrt[n]{C_0}$, donde C_0 representa el número de casos en el momento en que el comienza el recuento [131].

Si $p = 0$, esta ecuación diferencial describe una curva de incidencia constante en el tiempo, donde el número acumulado de casos crece linealmente. Por el contrario, se obtiene un modelo de dinámica de crecimiento exponencial si $p = 1$, siendo la solución de la ecuación $C(t) = C_0 e^{rt}$ es donde C_0 es el número inicial de casos. Al elegir valores intermedios de p entre 0 y 1, la ecuación describe un comportamiento de crecimiento sub-exponencial. Por ejemplo, para $p = 1/2$ la incidencia crece linealmente mientras que el número acumulado de casos sigue un polinomio cuadrático. Para $p = 2/3$ la incidencia crece de forma cuadrática mientras que el número acumulado de casos se ajusta a un polinomio cúbico. Este modelo también puede soportar diferentes patrones de crecimiento epidémico dependiendo del intervalo en el que se mueve el valor de p . Esto incluye patrones de incidencia lineal para $p = 0.5$, patrones de incidencia cóncavos para $0 > p > 0.5$ y patrones de incidencia convexos para $0.5 < p < 1$ [131].

4.5.2 Modelos epidémicos de crecimiento logístico

A pesar de que GGM proporciona una aproximación adecuada para la fase inicial o las primeras etapas de la propagación de una epidemia, este modelo no tiene en cuenta las reducciones en la incidencia de la enfermedad debido a las características del patógeno, la inmunidad de la población o la implementación de medidas médicas o sociales. Por lo tanto, considerar el crecimiento ilimitado dinámica de transmisión de una enfermedad es poco realista. Para resolver este problema, algunos modelos epidémicos consideran el crecimiento logístico, en el que, para una población estable dada, tendría un nivel de saturación que representa un límite superior numérico para el tamaño de crecimiento de la epidemia. Este límite se denomina típicamente capacidad de carga K y, en este modelo, representa el tamaño final de la epidemia. Este parámetro es fundamental para estimar la gravedad de la enfermedad, ya que representa el tamaño final de la población que se infectó. El GLGM se define mediante la siguiente ecuación diferencial [118]:

$$\frac{dC(t)}{dt} = C'(t) = rC^p(t) \left(1 - \frac{C(t)}{K}\right) \quad 4.48$$

donde $C(t)$ representa el número acumulado de casos en el tiempo t , r es la tasa de crecimiento intrínseco, p es la escalado del parámetro de crecimiento. Como en el modelo GGM, $p = 1$ indica un crecimiento exponencial temprano, mientras que $p = 0$ representa un crecimiento constante, y $0 < p < 1$ acomoda un polinomio o sub-exponencial temprano. $K > 0$ es la capacidad de carga o tamaño final de la epidemia, que representa el número total de población afectada. Este parámetro es crucial para generar pronósticos tras un pico epidémico y, además, puede vincularse a un parámetro de gran importancia modelos epidémicos clásicos como es el número reproductivo básico \mathcal{R}_0 , que representa la fase de transición del proceso de no equilibrio de propagación de una enfermedad. Este parámetro constituye un umbral epidemiológico clave en los sistemas biológicos ya que si $\mathcal{R}_0 < 1$ la infección se extingue mientras que si $\mathcal{R}_0 > 1$ puede causar una enfermedad epidémica. Por ejemplo, asumiendo que la evolución de un brote epidémico puede modelarse con el modelo epidémico básico SIR, el número reproductivo básico se puede calcular como $\mathcal{R}_0 = S_0/\rho$, donde S_0 es la población inicial de susceptibles, $\rho = (S_0 - S_\infty)/(\ln S_0 - \ln S_\infty)$, con S_∞ el número final de susceptibles, y $K = S_0 - S_\infty$ es el tamaño final de la epidemia.

4.6 Conclusiones

Con miras a darle solidez a esta Tesis, en este Capítulo se ha presentado un estudio de los modelos matemáticos más relevantes utilizados en epidemiología. Dentro de este amplio campo de estudio, en primer lugar, se han descrito varios modelos básicos dentro del grupo de los modelos denominados *mecanicistas*, definiendo primeramente conceptos básicos propios de la epidemiología, tales como el número reproductivo básico \mathcal{R}_0 , la incidencia acumulada, el número de susceptibles, infectados o recuperados, la tasa de mortalidad, o la tasa de contagio, entre otros.

Dentro de estos modelos *mecanicistas*, se ha profundizado en la formulación matemática del modelo *Susceptible, Infectado, Recuperado* (SIR). Este modelo, es

considerado como modelo básico en epidemiología, pero a la vez realmente versátil, en el estudio de enfermedades infecciosas. De igual forma, en este Capítulo se han mencionado, modelos más complejos que derivan del modelo SIR, aunque no de forma tan exhaustiva, donde se han incluido modelos que contemplan la vacunación de los individuos de la población, la cuarentena o la existencia de múltiples cepas de un mismo patógeno.

Por otra parte, también se han incluido en este Capítulo los modelos epidemiológicos, denominados *fenomenológicos*, los cuales suelen utilizarse para realizar predicciones a corto y medio plazo de la evolución de una enfermedad dentro de una población, tomando como referencia series de datos empíricos u observaciones al inicio de la epidemia. En este caso, se seleccionaron para el estudio el modelo de crecimiento exponencial (*Generalized Growth Model*, GGM) y el modelo de crecimiento logístico generalizado (*Generalized Logistic Growth Model*, GLGM).

Señalar que, los modelos epidemiológicos que se utilizarán para la fase de experimentación de esta Tesis, se aplican en el estudio las denominadas enfermedades infecciosas, ya que sus características de propagación (pueden ser transmitidas de un individuo a otro dentro de una determinada población, ya sea de forma directa o indirecta), hacen que la proximidad de un individuo sano a otro individuo infectado suponga un aumento significativo del riesgo o probabilidad de resultar también infectado. Este concepto de transmisión por proximidad en ausencia de contacto, se ajusta al modelo de comunicación inalámbrica utilizado en las redes a estudio.

CAPÍTULO

5

Materiales y métodos para la caracterización y análisis epidemiológico de la propagación de ataques *jamming*

En esta sección se describe el conjunto de materiales y métodos propuestos para el estudio de la propagación de los ataques *jamming* contra una red de sensores inalámbricos. Estos métodos se basan en el uso de modelos epidemiológicos de propagación de enfermedades cuyo principal vector de transmisión es el aire, y en las que su dinámica de propagación puede ser descrita mediante el uso de modelos deterministas y fenomenológicos, ambos soportados por el análisis de datos de referencia. El objetivo principal del modelado matemático de una enfermedad infecciosa, es describir el proceso de transmisión de la enfermedad una vez que uno o varios individuos infectados se introducen en una población de susceptibles, y la enfermedad empieza a propagarse en dicha población. Esta descripción se basa en la obtención de los parámetros principales que caracterizan la dinámica de propagación de la enfermedad. Este mismo principio se aplica para el análisis de la propagación de los ataques *jamming* en cada uno de los escenarios de propuestos.

Desde el punto de vista funcional, una red de sensores inalámbricos se caracteriza por hacer uso de la cooperación entre los nodos que la forman para crear rutas de comunicación inalámbricas. Las capas físicas (PHY) y de acceso al medio

(MAC) del protocolo de comunicación utilizado, pueden considerarse críticas en el proceso de transmisión, si bien las capas superiores pueden jugar también un papel importante en este proceso. Por otro lado, los dispositivos utilizados en estas redes están limitados en cuanto a sus capacidades de procesamiento, capacidad de memoria o autonomía de sus baterías. Si bien estas limitaciones pueden considerarse como una barrera natural contra ataques que requieran cierta complejidad, como por ejemplo la inyección de código, la propia naturaleza de la tecnología inalámbrica y del propio protocolo de comunicación utilizado, así como factores relacionados con el modo de despliegue de este tipo de redes, aumentan significativamente la probabilidad de ejecutar ataques tipo *jamming* cuyo objetivo es interferir intencionalmente el funcionamiento normal del medio inalámbrico, a nivel físico y de acceso, saturando el canal mediante la inyección continua o aleatoria de paquetes de datos (con o sin sentido), causando anomalías y errores en la transmisión de información entre los nodos dentro de la red.

5.1 Introducción

En el Capítulo 3 sobre fundamentos de Ciberseguridad en redes de sensores inalámbricos, se comentó que si bien algunos autores los agrupaban los ataques *jamming* como ataques de bloqueo de la capa de enlace [95], de acuerdo con la taxonomía propuestas recientemente, y en especial la propuesta por Lichtman [96], los ataques *jamming* entran dentro de la categoría de ciberataques y están generalmente relacionados con los ataques de denegación de servicio (DoS). También se vio que un atacante podía usar varias estrategias con diferentes niveles de eficiencia, para llevar a cabo tales ataques contra las capas física (PHY) y de acceso al medio (MAC), siendo las más habituales la generación continuada de paquetes de datos a una determinada tasa (*jamming* constante), y la generación aleatoria de paquetes de datos (*jamming* aleatorio).

Desde el punto de vista de la epidemiología, se define una enfermedad infecciosa como aquella que es capaz de provocar un conjunto de disfunciones en cualquiera de los sistemas del cuerpo, identificables por un patrón conocido de signos y síntomas relacionados a lo largo del tiempo, dentro de una población, y que además puede transmitirse, directa o indirectamente, de una persona a otra [102]. En este sentido, se establece el número reproductivo básico \mathcal{R}_0 como un parámetro clave para

entender la dinámica de la propagación de una enfermedad y de su brote epidémico, ya que, por una parte, representa el número de casos secundarios esperados producidos por un único individuo infectado introducido en una población completamente susceptible; y por otra, permite analizar la estabilidad local del estado libre de enfermedad (*Disease Free Equilibrium*, DFE). En otras palabras, a medida que \mathcal{R}_0 aumenta y se aleja del valor umbral crítico, el DFE pierde su estabilidad, acercándose el sistema a un punto de equilibrio próximo al equilibrio endémico (*Endemic Equilibrium*, EE). Además, desde el punto de vista epidemiológico, este equilibrio requiere una aportación continua de individuos susceptibles dentro de la población, ya sea por nacimientos o por pérdida de inmunidad ante la infección. Por el contrario, sin aportación continua de individuos susceptibles, cuando el sistema se aproxima al punto de equilibrio endémico, el número de infectados siempre vuelve a cero una vez que el brote epidémico ha finalizado. En esta situación, si dentro de una población individuos susceptibles se introducen uno o más individuos infectados, entonces la enfermedad en cuestión comenzará a propagarse de los individuos infectados a los susceptibles, haciendo que la población de susceptibles descienda a la vez que aumenta la de infectados, hasta alcanzar un pico máximo. Posteriormente, los infectados comenzarán a recuperarse, hasta que finalmente, y tras un determinado periodo de tiempo, el brote epidémico desaparece de la población, quedando un número determinado de susceptibles sin infectar, ningún infectado y un número determinado de recuperados. Este brote epidémico será de mayor intensidad (mayor número de infectados, mayor duración, etc.), cuanto más se aleje el sistema del punto de equilibrio libre de enfermedad DFE, esto es, cuanto mayor sea \mathcal{R}_0 .

Trasladando estos conceptos al modelo de ataque *jamming*, para el desarrollo de esta tesis se asume que, dentro de una red de sensores inalámbricos con una población fija en la que inicialmente se considera que todos los nodos pertenecen al grupo de individuos susceptibles, se introduce un nodo infectado (*el paciente cero*) que será el nodo *jammer*. Este nodo que porta la enfermedad o agente infeccioso comenzará un ataque tipo *jamming* mediante la generación paquetes de datos ya sea de forma continua o aleatoria. Para fines de modelado, el efecto producido por el ataque *jamming* sobre los nodos se considerará como un tipo de enfermedad infecciosa cuyo medio de transmisión principal es el aire, y que provocará una serie de disfunciones en estos nodos, identificables por un patrón conocido de signos y síntomas relacionados a lo largo del tiempo, con el potencial añadido de afectar progresivamente a otros nodos de la red.

Esto es, en principio el ataque comenzará afectando a los nodos más próximos al atacante y, pasará de estos a otros nodos para ir propagándose a través de la red. Esta propagación del ataque se deberá, fundamentalmente, a la saturación del canal de comunicación a nivel físico y a otros efectos negativos provocados en el tráfico de red inducidos en la capa de acceso al medio, tales como el aumento de las colisiones. Los síntomas del ataque comenzarán a manifestarse en primer lugar en los nodos afectados más próximos al atacante, a través de un aumento en el número de paquetes reenviados entre nodos, la pérdida de paquetes de datos, el uso excesivo de recursos como la memoria, el tiempo de procesamiento, entre otros; y en última instancia, podría provocar el agotamiento de las baterías. En conjunto, todos o parte de estos síntomas causarán que los nodos afectados no sean capaces de comunicarse con el resto de los nodos de la red. Posteriormente, esos mismos síntomas comenzarán a observarse en los nodos próximos a los primeros nodos infectados, ya que éstos tendrán dificultades en comunicarse entre ellos. Este efecto se irá propagando a través de la red, siendo mayor la incidencia en la población de nodos cuanto mayor sea el número reproductivo básico \mathcal{R}_0 asociado al ataque. Esta mayor incidencia se reflejará en un mayor número de nodos afectados y una mayor duración del ataque. Cabe señalar que, en este modelo los nodos que superan la enfermedad (el ataque *jamming*) se considerarán totalmente recuperados de la infección (han adquirido inmunidad frente al ataque) y, por lo tanto, dejarán de participar en la propagación del ataque, incluso cuando se comuniquen con otros nodos.

5.2 El conjunto de datos

Dentro de los estudios epidemiológicos, la validación de un determinado modelo matemático mediante la utilización de datos existentes sobre una enfermedad o un brote epidémico es un factor clave, ya que proporciona una prueba sobre fiabilidad de las hipótesis de modelado adoptadas y permite, en su caso, realizar predicciones sobre la dinámica de dicha enfermedad o brote epidémico a corto o medio plazo. Sin embargo, esta validación puede ser difícil de realizar y dependerá en gran medida de la disponibilidad y calidad de los datos. Por ejemplo, es posible que el conjunto de datos existente sobre un brote epidémico no esté completo, no sean lo suficientemente preciso, exista dispersión de los casos reportados, o incluso que haya que esperar a la finalización del brote para que el análisis estadístico sea confiable. La validación de los

resultados de los diferentes modelos epidemiológicos propuestos en esta tesis para la caracterización y análisis de la propagación de ataques *jamming* en redes de sensores inalámbricas, también depende, por tanto, de la disponibilidad y calidad de datos asociados a este tipo de ataques. Si bien en la literatura reciente pueden encontrarse referencias a los efectos de los ataques *jamming* contra redes de sensores inalámbricos, [58], [59], [60], [61], [62], [134], [135], en la mayoría de estos trabajos los datos proporcionados no resultan útiles para realizar una validación adecuada de los modelos propuestos. Por una parte, en algunos casos los escenarios de prueba utilizados, ya sean basados en simuladores o en la implementación física de redes inalámbricas, contemplan un número de nodos a estudio es muy reducido ofreciendo, por tanto, un número muy limitado de muestras sobre los efectos del ataque. En otros casos los datos obtenidos en los diferentes escenarios de prueba propuestos, aportan información sobre parámetros de degradación del canal de comunicación como el número de reintentos de conexión en la capa de acceso al medio (MAC); parámetros sobre la tasa de error en la transmisión de datos tales como el error bit (*Bit Error Rate*, BER), número de paquetes retransmitidos o perdidos (*Packet Error Rate*, PER); o bien parámetros relacionados con el consumo de energía y de tiempo de ejecución de aplicaciones en los nodos. Sin embargo, dentro de este grupo de trabajos de investigación resulta de especial interés los datos obtenidos en [22], donde se llevaron a cabo varias simulaciones que reproducían fielmente el funcionamiento de los protocolos de enrutamiento utilizados [136], [137]. Con estas simulaciones, se trataba de estudiar los efectos causados al lanzar ataques *jamming*, en concreto de tipo aleatorio y de tipo reactivo, contra una red de sensores trabajando bajo tres protocolos de enrutamiento diferentes, y considerando además tres escenarios, tomando en cada uno de ellos una ubicación diferente para el nodo atacante. La simulación de referencia, considera una red ad-hoc con nodos estáticos, y un único nodo coordinador de red que recopilaba toda la información generada por el resto de los nodos de la red. Este tipo de implementaciones, puede encontrarse en un gran número de aplicaciones de redes de sensores inalámbricos, tal y como se describió en el Capítulo 2 sobre fundamentos sobre redes de sensores inalámbricos.

Como se indica al inicio de este mismo Capítulo, para fines de modelado, el efecto producido por el ataque *jamming* sobre los nodos se considerará como una enfermedad infecciosa cuyo medio de transmisión principal es el aire, y que provoca disfunciones en estos nodos, con un patrón conocido síntomas a lo largo del tiempo. En

este sentido, Wood y Stankovic [68] identifican el ataque *jamming* como un caso especial de ataque denegación de servicio (DoS) y lo definen como *cualquier evento que disminuya o elimine capacidad de la red para realizar su función esperada*, definición que puede relacionarse con el concepto de enfermedad infecciosa descrito con anterioridad. Esta disminución o eliminación de la funcionalidad de la red, vendrá provocada por la disfunción en los nodos, cuyos primeros síntomas al inicio del ataque comenzarán a manifestarse en los nodos más próximos al atacante, con aumento generalizado del consumo de recursos debido, por ejemplo, al esfuerzo extra en la retransmisión de paquetes o en el procesado de errores. En última instancia, esa situación podría provocar el agotamiento de las baterías de los nodos. En conjunto, todos o parte de estos síntomas irán propagándose por el medio inalámbrico, causando que un número importante de los nodos afectados resulten inalcanzables por el coordinador, o que éstos no puedan comunicarse con el resto de los nodos de la red, dejando ésta de realizar sus funciones.

Para la validación de los resultados de los diferentes modelos epidemiológicos para la caracterización y análisis de la propagación de ataques *jamming* en redes de sensores inalámbricas, se tomarán como base la arquitectura propuesta en [22], consistente en una red de sensores inalámbricos con 49 nodos estáticos distribuidos uniformemente en un área de 300x300 metros. En la Figura 5.1. puede verse representado un ejemplo de la arquitectura de red inalámbrica de referencia. Del total de nodos, el nodo ubicado en la esquina superior izquierda actúa como coordinador, y los otros 48 nodos restantes recopilan la información que es enviada a dicho coordinador con una tasa de 1%–4% paquetes por segundo. En adelante, los datos proporcionados por estas simulaciones serán mencionados como los *datos de referencia*.

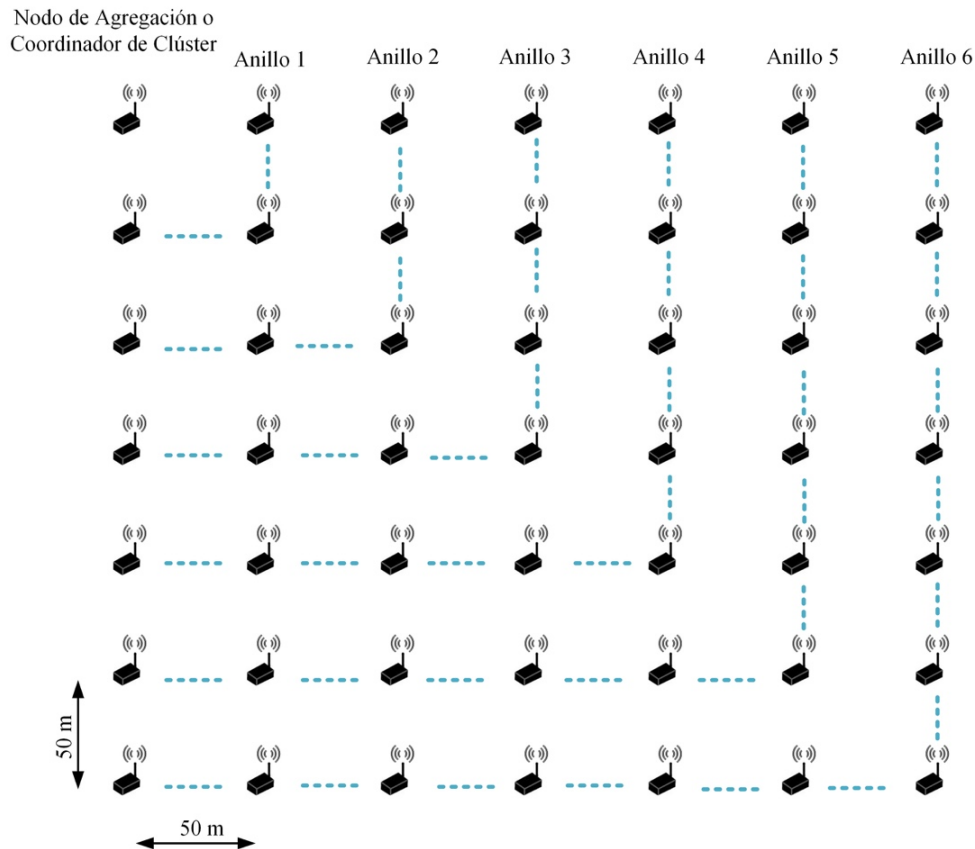


Figura 5.1. Topología de la red del escenario a estudio.

Más específicamente, este trabajo se centraba en recopilar datos relevantes sobre cómo se degrada el rendimiento de la red inalámbrica bajo los efectos del ataque jamming, utilizando tres protocolos de enrutamiento diferentes que desempeñan funciones de autoconfiguración de la red: *Ad-hoc On-demand Distance Vector* (AODV) [53], *Dynamic Source Routing* (DSR) [54] y *Multi-Parent Hierarchical Protocol* (MPH) [55], cuyos fundamentos se expusieron en el Capítulo 2. En la capa de acceso al medio (MAC), se dispuso del protocolo CSMA/CA (*Carrier Sense Multiple Access with Collision Avoidance*), con un máximo de tres retransmisiones por paquete y un máximo de cinco reintentos CSMA, mientras los nodos esperan que el canal esté inactivo antes de la transmisión. Por otra parte, a nivel físico se adoptó el chip CC2530 [138] que según el estándar IEEE 802.15.4, considera una potencia radiada de 0 dBm y una potencia de señal recibida -85 dBm, con lo que se obtiene un radio de cobertura medio para los nodos de 50 m. En la Tabla 5.1 se presentan parámetros principales utilizados en la simulación [22].

Parámetro	Valor
Capa física (PHY)	
Umbral de sensibilidad	-78 to -94 dBm
Potencia de transmisión	0 dBm
Radio de cobertura medio	50 m
Capa de acceso al medio (MAC)	
Número máximo de retransmisiones	3
Número máximo de reintentos para alcanzar a un nodo desde el coordinador	9
Tasa de error de paquetes	1% – 4%
Longitud media de trama	22 bytes
Número máximo de retrocesos (<i>backoff</i>)	4
Protocolo MAC	IEEE 802.15.4
Capa MAC	CSMA/CA
Capa de red	
Número de nodos	49
Tiempo de descubrimiento de nodo vecino	10 s
Tasa máxima de transmisión	250 kbps
Topología	Malla de nodos estáticos, 300x300 m

Tabla 5.1. Principales parámetros usados en el entorno de simulación.

Para efectos del estudio, se consideró que el nodo atacante poseía las mismas características hardware y software que el resto de los nodos, mientras que el nodo coordinador, disponía recursos ilimitados en cuanto a capacidad de procesamiento, baterías, etc., por lo que se considera “inmune” al ataque *jamming*.

5.2.1 Modelos de ataques *jamming*

Si bien en el Capítulo 3 sobre fundamentos de ciberseguridad en redes de sensores inalámbricos, se describieron los distintos tipos de *jamming* dentro de la clasificación de los ataques a redes de sensores inalámbricos. En este apartado se presenta a modo de recordatorio, las características fundamentales de las estrategias de ataque utilizadas en [22], donde se utilizan dos estrategias de ataque *jamming*: aleatorio y reactivo. El *jamming* aleatorio es, por un lado, uno de los tipos de ataque más simples de implementar y bastante difícil de detectar. Por otro lado, el *jamming* reactivo es complejo de implementar, pero mucho más difícil de detectar.

Para el caso del *jamming* aleatorio, el nodo *jammer* transmite una serie de paquetes por segundo siguiendo una distribución uniforme, pudiendo ajustarse la tasa de paquetes para aumentar o reducir el nivel de agresividad del ataque. Una baja tasa de paquetes por segundo, representa una actividad de *jamming* reducida y, como consecuencia un ataque, por ejemplo, de tipo DoS (*Denial of Services*), no se ejecutará de forma continuada. Sin embargo, desde el punto de vista de la detección, sería bastante difícil identificar este ataque, ya que sus efectos podrían confundirse con una interferencia normal debido al propio entorno inalámbrico. De forma análoga, una tasa alta de paquetes por segundo producirá efectos más severos, considerándose como la situación más desfavorable para la red inalámbrica en términos de degradación del rendimiento. En el escenario de pruebas se usaron tasas de 50 a 80 paquetes/s, para observar el comportamiento de la red.

En el caso del *jamming* reactivo, se aplica una estrategia de ataque en la que el nodo genera y transmite un paquete con el objeto de generar colisiones en la capa MAC con los paquetes legítimos. En esta situación, el nodo *jammer* monitoriza el medio inalámbrico, y una vez detecta un paquete, transmite el suyo generando una colisión en el medio. El *jammer* conseguirá tener éxito con el ataque si es capaz de alterar al menos un bit del paquete original, y además sólo se implementa un mecanismo de detección de errores, pero no de corrección de éstos. Esta estrategia de ataque utiliza menos energía que la estrategia de *jamming* aleatorio, además es quizás uno de los ataques más difíciles de detectar ya que el nodo atacante está observando el canal inalámbrico mediante una escucha pasiva (*eavesdropping*) y sólo actúa para provocar las colisiones.

5.3 Pre-procesamiento de los datos

Dentro del conjunto de datos obtenidos en [22], son de especial interés para el desarrollo de esta tesis el número de nodos inalcanzables por el coordinador para cada una de las ubicaciones del nodo *jammer* y tipo de ataque, teniendo en cuenta, además, el tipo de protocolo de enrutamiento utilizado. De este modo se obtienen un total de 27 simulaciones diferentes, aportando unos 2700 puntos de muestreo temporal. Dado que los datos de referencia proporcionados inicialmente no permiten realizar una comparación directa con los diferentes apartados del estudio epidemiológico

experimental presentado en esta Tesis, en primer lugar, se ha procedido al pre-procesamiento de los datos.

En una población, la resistencia frente a un determinado patógeno depende de factores intrínsecos a dicha población relacionados especialmente con su capacidad inmunitaria. En el caso de una red de sensores inalámbricos, la resistencia frente a cierto tipo de ataques puede considerarse intrínsecamente relacionada con los protocolos de comunicación utilizados. Dado que a nivel de capa física y de acceso al medio todos los escenarios utilizan el estándar IEEE 802.15.4, la resistencia frente al ataque será diferente dependiendo del protocolo de enrutamiento utilizado. Por lo tanto, para efectos de simulación y análisis, se asume que se dispone de tres poblaciones de nodos sensores, donde en cada una de ellas se equipa a dichos nodos con un protocolo de red diferente: AODV, DSR o MPH. Además, para el desarrollo comparativo presentado en esta Tesis, se puede asumir que las poblaciones de nodos se enfrentan a dos tipos de patógenos de una misma familia y que provocará, en principio, enfermedades similares pero con síntomas ligeramente diferentes. Por una parte, se tiene el ataque aleatorio del que se dispone además de dos cepas, una que actúa a una tasa de 50 paquetes/s, y otra que lo hace a 80 paquetes/s; y, por otra parte, se tendrá un ataque reactivo el cual se ejecuta de forma distinta a los anteriores. Esta distinción aporta consonancia con los modelos epidemiológicos.

A modo de resumen, para la obtención del conjunto de datos de interés relacionados con los intentos de conexión desde el coordinador a cada nodo en [22], se estableció un periodo de 100 segundos durante el que la red se mantenía en funcionamiento normal. Posteriormente se introdujo un nodo *jammer* y se mantuvo en la red otros 100 segundos. Durante este tiempo, el nodo coordinador lanzaba peticiones de alcance (*ping*) a cada uno de los nodos de la red, constituyendo aproximadamente 20 repeticiones del proceso durante el período 100 segundos. Los nodos alcanzables por el coordinador se definen, por tanto, como el número de nodos que pueden responder a las peticiones del coordinador. Idealmente, el coordinador debe conocer toda la topología de la red y, por lo tanto, debe poder llegar a todos los nodos cuando sea necesario [22]. Si para el escenario propuesto se toma $N = 49$, como el número total de nodos, $S(0) = 48$ como el número de nodos que inicialmente están en disposición de comunicarse con el nodo coordinador, y $A(t)$ como el número de nodos alcanzados por el coordinador, podemos definir las siguientes relaciones. El número de nodos inalcanzables $I(t)$ o

afectados por el ataque en cada instante t puede obtenerse como $I(t) = S(0) - A(t)$; mientras que el número acumulado de nodos inalcanzables o afectados en el tiempo t , se obtiene como $C(t) = \sum_{i=1}^t I(t)$. Haciendo uso de estas relaciones se puede obtener el conjunto de datos necesario para cada uno de los modelos epidemiológicos a estudio. Por otra parte, también es preciso definir el intervalo de tiempo de estudio de la epidemia o ataque. El tiempo inicial vendrá dado por el instante $t = 0$, en el que se introduce en la red el nodo *jammer* o *paciente cero*, donde la población de nodos está compuesta por un nodo infectado, $S(0) = 48$ nodos susceptibles, $R(0) = 0$ nodos recuperados, $D(0) = 0$ nodos caídos y $C(0) = 0$ nodos acumulados. Por tanto, el vector de población inicial tendrá la forma $\{S, I, R, D\} = \{48, 1, 0, 0\}$. Si además se tiene en cuenta que según se indica en los datos de referencia, el tiempo necesario para descubrir a cada de nodo vecino es de 10 segundos, este es el intervalo de muestreo para determinar cómo varía la población durante el ataque. Finalmente, aunque en los datos de referencia sólo se establece un marco temporal de ataque de 100 segundos, para el conjunto de experimentos se ha generado un periodo de ataque de entre 150 y 180 segundos, asumiendo que en este instante la red ha alcanzado el estado estacionario. A modo de ejemplo, en la Tabla 5.2 se presentan los datos de interés relativos al ataque *jamming* aleatorio a 50 paquetes/s realizado por un nodo atacante ubicado en un punto intermedio de la topología de la red, cuando los nodos incorporan el protocolo de enrutamiento AODV. Como se señaló anteriormente, y según se indica en los datos de referencia, se asume que para un total de $N = 49$ nodos que integran la red, 48 de ellos son susceptibles al ataque.

Las celdas sombreadas de la tabla corresponden al intervalo de tiempo que contiene los datos procesados, teniendo en cuenta la información proporcionados por los datos de referencia, mientras que el resto de los datos se han añadido al modelo para completar los 150 segundos de simulación. Las tablas correspondientes al resto de los casos de ataques *jamming* para cada uno de los escenarios expuestos en [22] se presentan en el Apéndice II.

Tiempo (s)	Nodos Inalcanzables $I(t)$	Inalcanzables Acumulados $C(t)$	Nodos susceptibles $S(t)$	Nodos Recuperados $R(t)$	Nodos Caídos $D(t)$	Nodos Alcanzados $A(t)$
0	1	0	48	0	0	48
10	4	4	44	0	0	44
20	1	5	43	4	0	47
30	1	6	42	5	0	47
40	4	10	38	6	0	44
50	8	18	30	10	0	40
60	8	26	22	18	0	40
70	7	33	15	26	0	41
80	3	36	12	33	0	45
90	1	37	11	36	0	47
100	0	37	11	36	1	47
110	0	37	11	36	1	47
120	0	37	11	36	1	47
130	0	37	11	36	1	47
140	0	37	11	36	1	47
150	0	37	11	36	1	47

Tabla 5.2. Resultado simulado de un ataque *jamming* aleatorio a 50 paquetes/s contra una red con protocolo de enrutamiento AODV, cuando el nodo atacante se ubica centrado en la topología de red.

5.4 Modelado de la red de sensores inalámbricos

Uno de los aspectos que se suele destacar en epidemiología es que los patrones por los cuales las enfermedades se propagan a través de la población están determinados no solo por las propiedades del patógeno que la provoca (capacidad de contagio, la duración de su período infeccioso, gravedad, etc.) sino también por factores demográficos de la población a la que está afectando. Tal y como se indicó en el Capítulo 4, los modelos epidémicos más habituales, ya sean básicos o complejos, asumen que la población está bien mezclada, por lo que cualquier pareja de individuos tiene la misma probabilidad de interactuar entre sí durante un intervalo de tiempo determinado. Esta asunción, presupone que cualquier individuo infectado tiene la misma probabilidad de contagiar la enfermedad a cualquier otro individuo susceptible con el que contacte y, además, que todos los contactos transmiten la enfermedad con la misma probabilidad. Para poblaciones de gran tamaño, esta suposición permite describir la dinámica de los modelos epidémicos mediante sistemas de ecuaciones diferenciales ordinarias de las que se pueden obtener soluciones de interés, como el número máximo de infectados, el número reproductivo básico y si se producirá o no un brote epidémico. Sin embargo, esta hipótesis si bien permite obtener resultados válidos en los estados

iniciales de un brote epidémico, también hace que en algunos casos se obtenga un sobredimensionamiento en la estimación de los valores de la epidemia, tales y como sucedió con el brote de SARS entre 2002 y 2003 [139]. En este sentido, la adopción de modelos epidémicos basados en redes proporciona una forma alternativa de describir una población, así como las interacciones entre los individuos que la componen. En estos modelos, los vértices de la red representan individuos que se conectan unos con otros mediante aristas, representando así las interacciones entre individuos que podrían conducir a la transmisión una enfermedad o infección. Es interesante observar que este enfoque utilizado en epidemiología, se emplea habitualmente para representaciones de redes similares en otros contextos, como son las redes de transporte, redes de telecomunicaciones incluyendo Internet y la *World Wide Web* y redes sociales [140].

Uno de los métodos para modelar una epidemia incluyendo la estructura de red sobre la que se propaga, consiste en descomponer la tasa de contagio de un modelo epidémico clásico, en dos parámetros. Uno de estos parámetros refleja la tasa promedio de contactos entre individuos susceptibles e infectados, y el otro parámetro denominado transmisibilidad, representa la probabilidad de que la infección se haga efectiva dado el contacto entre un individuo susceptible y un infectado [140], [141]. Esta idea, ya se discutió en el Capítulo 4, cuando se habló del número reproductivo básico \mathcal{R}_0 , donde la tasa de infección o contagio β se descomponía en los parámetros τ y \bar{c} , donde τ es la transmisibilidad, dependiente del agente infeccioso, y representa la probabilidad de que se produzca una infección dado el contacto entre un individuo susceptible y un individuo infectado; mientras que \bar{c} es la tasa promedio de contacto entre individuos susceptibles e infectados. En base al modelo SIR, se puede asumir que existe la probabilidad de que se produzcan conexiones entre pares de individuos infectados y susceptibles (nodo *jammer* y nodos sensores), que predisponen a estos últimos al contacto que causa la enfermedad, aunque no se garantiza que se produzca un contagio efectivo. De este modo, la tasa de contagio β puede descomponerse en dos parámetros, siendo k el número promedio de conexiones entre nodos que representa, por tanto, la tasa promedio de contactos entre individuos susceptibles, e infectados. Por otra parte, la transmisibilidad λ , representa la probabilidad de que el ataque *jamming* sea efectivo dado el contacto entre un susceptible y un infectado, siendo la tasa de contagio para este modelo $\beta = \lambda \cdot k$. Al igual que en los modelos epidémicos, el valor de k dependerá de la distribución de los nodos, mientras que λ dependerá de las características del ataque.

Para determinar el valor de k , considérese una red de sensores inalámbricos compuesta por un conjunto de N nodos idénticos, distribuidos independientemente de forma aleatoria y uniforme, en un área bidimensional A , tal que la densidad media puede considerarse como $\rho = N/A$. Cada nodo utilizará el estándar IEEE 802.15.4 el cual define la capa física y la capa de acceso al medio de la comunicación inalámbrica. A modo de recordatorio, la capa física (PHY) define aspectos tales como las bandas de frecuencia, canales y velocidad de datos; además es responsable de la activación y desactivación del transceptor de radio, la medición de la calidad del enlace, la evaluación clara del canal y la selección del canal. Por otra parte, la capa de acceso al medio (MAC) ofrece una interfaz de administración y señalización de red para acceder al canal físico. La transmisión inalámbrica entre los nodos dentro de la red, se asume como un modelo de enlace de radio en el que cada nodo está equipado con una antena omnidireccional que se rige por el modelo de pérdidas en el espacio libre (*Free-Space Path Loss*, FSPL) dada por la Ecuación de Transmisión de Friis [142], y con un rango de transmisión máximo r_0 .

Suponiendo una distribución uniforme de nodos, la probabilidad de que el ataque afecte a un nodo específico dentro del área A vendrá dada por $p = \pi r_0^2 / A$, donde p representa la probabilidad de existencia de un enlace en el nivel físico, es decir, que al menos dos nodos estén dentro de su rango de comunicación. Por otra parte, la probabilidad de que el ataque no afecte a ese nodo específico es $(1-p)$, la probabilidad de que el ataque no afecte a ninguno de los N nodos de la red es $P_{NA} = (1-p)^N$, y la probabilidad de que el ataque afecte al menos a un nodo es $P_A = k = 1 - P_{NA} = 1 - (1-p)^N$, que para la red descrita se puede aproximar como $k = 1 - e^{-Np}$ [143]. Por lo tanto, k representa la tasa promedio de contactos entre nodos susceptibles y afectados. Fijados estos parámetros para la red a estudio, se obtiene que $k \approx 0.9848$. De este modo, se puede estimar el valor de la tasa de contagio β como el número de contactos efectivos por unidad de tiempo $\beta = \lambda \cdot k = \lambda(1 - e^{-Np})$, siendo λ la probabilidad de que el ataque sea efectivo dado el contacto entre un nodo susceptible y un nodo afectado. Esta formulación de β también permite que el modelo propuesto esté de acuerdo con la definición de enfermedades infecciosas desde el punto de vista epidemiológico, ya que éstas se caracterizan porque pueden transmitirse, directa o indirectamente, de un individuo a otro dentro de una población, por lo que la proximidad de un individuo sano a otro infectado supondrá un aumento significativo en el riesgo de contagio.

Cabe destacar como veremos posteriormente que, en el caso de los modelos *fenomenológicos* basados en crecimiento de poblaciones, no es preciso definir los parámetros relacionados con la tasa de contagio.

5.5 Definición de los grupos de individuos en la población de nodos sensores

Si bien, como se ha visto en el Capítulo 4, en la mayoría de los modelos epidemiológicos clásicos, los individuos dentro de la población se dividen de acuerdo con su capacidad de transmitir la enfermedad, en otros modelos se adopta la filosofía utilizada en medicina, donde estos individuos se agrupan de acuerdo con el estado de afectación en que se encuentran en relación dicha enfermedad. Para el desarrollo de esta Tesis, se adoptará este enfoque de estado frente a la enfermedad de los nodos, aplicándolo tanto a los modelos de tipo *mecanicistas* como a los modelos *fenomenológicos* de propagación del ataque, permitiendo así identificar los parámetros clave asociados a dicho ataque. En este caso se asume que, si bien los nodos afectados por el primer nodo infectado (nodo *jammer*) o *paciente cero* no se convierten *de facto* en otros nodos *jammer*, sí contribuyen de forma directa y activa a la propagación del ataque. Por lo tanto, la población de nodos a estudio puede agruparse, siguiendo un modelo epidemiológico, en *nodos susceptibles*, *nodos inalcanzables* o *afectados*, *nodos recuperados* y *nodos caídos*. Tomando como referencia el modelo epidémico SIR, la Figura 5.2 representa dinámica de propagación del ataque según los grupos de nodos propuestos.

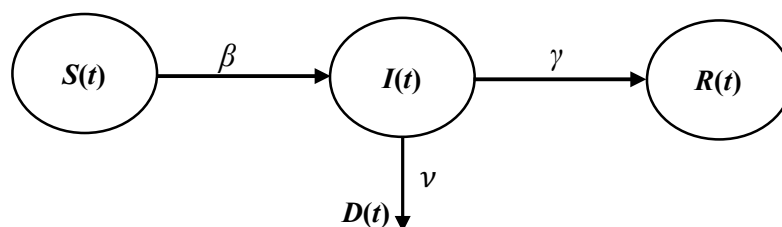


Figura 5.2. Dinámica propuesta de propagación del ataque *jamming*.

Cabe señalar en este punto que, al inicio de esta investigación, se propuso el modelo SEIS (Susceptible, Expuesto, Infectado y Susceptible), como modelo epidémico de referencia para la caracterización de la propagación de ataques *jamming* [17], [18]. Sin embargo, tras realizar los primeros estudios simulados usando los datos de referencia, se comprobó que el comportamiento dinámico de la red ante un ataque *jamming* se asemejaba más a un modelo SIR [19]. Por una parte, se observó que, debido a la velocidad con la que se producen las transmisiones dentro de la red, no tenía sentido contemplar un tiempo o periodo de latencia para los nodos Expuestos, ya que este tiempo sería prácticamente inapreciable con respecto a parámetros como la tasa de contagio o el tiempo de recuperación. Por otro lado, dado que los nodos incorporan protocolos de enrutamiento en capas superiores, éstos actúan de algún modo como un sistema inmunológico, permitiendo recuperar la comunicación a través rutas alternativas. De este modo, una vez que los nodos establecen esas nuevas rutas, y siempre que sea posible, permanecerán en el grupo de los recuperados, ya que no están afectados por el ataque y además no son propagadores de éste. Tal situación debería mantenerse, al menos, mientras no se produzca un ataque en otra zona de la red, o mientras no se provoque un tipo diferente de ataque [20, 21].

Siguiendo, por tanto, la dinámica de propagación indicada en la figura anterior, la población de N nodos sensores estará compuesta en cada instante de tiempo, por un grupo de nodos susceptibles $S(t)$ que, en principio, no se ven afectados por el ataque y, por lo tanto, pueden realizar normalmente sus funciones dentro de la red. Estos nodos podrían verse afectados y *enfermar* siendo inalcanzables por el coordinador, si entran en contacto con el atacante (*jammer*) o con nodos próximos a éste, a una tasa de contagio β . El siguiente grupo de la población, vendría dado precisamente por los nodos inalcanzables $I(t)$ y representan a aquellos nodos se ven afectados por el ataque después de estar en contacto con el nodo *jammer* o con otros nodos próximos a éste. Estos nodos presentan síntomas característicos observables tales como el aumento considerable en la tasa de paquetes erróneos recibidos (*Packet Error Ratio*, PER), aumento del número de paquetes reenviados, aumento en la pérdida de paquetes de datos, o el consumo adicional de recursos tales como memoria, tiempo de procesamiento, e incluso el agotamiento total de sus baterías. Estos síntomas incapacitarán y/o dificultarán a los nodos afectados que realicen con normalidad las funciones de comunicación en la red. Los nodos afectados o inalcanzables $I(t)$ pasarán al grupo de nodos recuperados $R(t)$ tras

un tiempo $t_r = 1/\gamma$ una vez superen el ataque. Si definimos $A(t)$ como el número de nodos alcanzados por el coordinador en cada instante t , donde $A(t) = S(t) + R(t)$, entonces el número de nodos inalcanzables $I(t)$ puede obtenerse fácilmente mediante la diferencia $I(t) = N - A(t)$. A su vez, el número acumulado de nodos inalcanzables o afectados en el tiempo t , se define como $C(t) = \sum_{i=1}^t I(i)$. Es fácil deducir, que para una población constante de N nodos, el número de susceptibles en cada instante vendrá dado por la expresión $S(t) = N - C(t)$. Finalmente, los ya mencionados nodos recuperados $R(t)$, representan el conjunto de nodos que una vez superado el ataque vuelven a poder realizar sus funciones dentro de la red y que, además de acuerdo con el modelo epidémico SIR, ya no participarán en la propagación del ataque, al haber desarrollado defensas contra este.

Además, y en aras de dotar de mayor aplicabilidad al marco de trabajo propuesto, se define el grupo de los nodos caídos $D(t)$ o *dropped nodes*, que representa a aquellos nodos que no consiguen recuperarse del ataque debido, por ejemplo, al agotamiento total de sus baterías, a una sobrecarga de procesamiento irreversible, etc. Este grupo es equivalente a los fallecimientos reportados en los modelos utilizados en epidemiología. El paso de los nodos afectados $I(t)$ al grupo $D(t)$, vendrá definida por la tasa de caída ν , que puede obtenerse partiendo de la Tasa de Fatalidad de Caso (*Case Fatality Rate*, CFR) y del tiempo medio de caída de los nodos. La tasa CFR se define como el cociente del número total fallecimientos entre el número total de individuos infectados [144] que, para el caso de la red de sensores inalámbricos, vendrá dada por el cociente $X = D(t)/I(t)$. Para $D(t) = X = 0$, se tiene el modelo SIR básico; y para una CFR dada X , la tasa de caída de los nodos será $\nu = X/t_D$, con t_D el tiempo medio que transcurre desde que un nodo afectado por el ataque deja de funcionar completamente. De forma análoga, se puede definir la tasa o periodo de recuperación como $\gamma = (1-X)/t_R$, siendo t_R el tiempo medio que dicho nodo tardaría en recuperarse del ataque. La suposición de una tasa de recuperación y caída de nodos constante es equivalente a asumir que los periodos de recuperación y caída durante el ataque, se distribuyen exponencialmente, con una media igual a $1/\gamma$ y $1/\nu$ respectivamente. Finalmente, con estas relaciones, la población de nodos queda definida en cada instante t , por $N = S(t) + I(t) + R(t) + D(t)$.

En el caso del segundo enfoque, caso de los modelos *fenomenológicos*, los nodos se agrupan de acuerdo con el estado de afectación en que se encuentran en relación al ataque *jamming*. Se asume, por tanto, que los nodos inalcanzables presentan

los síntomas inequívocos de que está siendo afectado por el ataque *jamming*, por lo que serán reportados como un caso positivo, siendo $C'(t)$ la incidencia o número de nodos afectados para cada instante t , dada por $dI(t)/dt = C'(t) = N - A(t)$. Por otra parte, el número acumulado de nodos inalcanzables o afectados en cada instante t será $C(t)$. Al igual que para el caso anterior, es fácil deducir, que para una población constante de N nodos, el número de susceptibles en cada instante vendrá dado por $S(t) = N - C(t)$.

5.6 Modelo SIR determinista para el estudio de la propagación de ataques *jamming*

El objetivo buscado con el modelo epidémico SIR es caracterizar y analizar la propagación del ataque, basándose en los parámetros fundamentales de este modelo, que han de ser, al menos la tasa de contagio o infección β y la tasa o periodo de recuperación γ . La obtención de estos parámetros permitirá representar las curvas de propagación del ataque, y a su vez, conformarán el número reproductivo básico del sistema \mathcal{R}_0 . Este número marcará la diferencia entre un proceso epidémico en el que el ataque se propagará a través de la red produciendo un número importante de contagios y con cierta rapidez; o un proceso no epidémico, en el que el ataque se extinguirá por sí sólo produciendo un número muy reducido de contagios. Estos parámetros también servirán como métricas para evaluar la incidencia del ataque. Por ejemplo, tanto el número reproductivo básico del sistema \mathcal{R}_0 , como la tasa de contagio o infección β puede tomarse como indicativos de la *severidad del ataque*, pues al igual que en los modelos epidémicos, permitirá reflejar el número promedio de nodos afectados que se producirá cuando un nodo afectado entre en contacto con otros nodos susceptibles. Por otra parte, el parámetro $1/\gamma$ permitirá conocer la *persistencia del ataque*, ya que representa el tiempo medio en el que un nodo inalcanzable permanece afectado por dicho ataque o de forma equivalente, el tiempo medio en el que el nodo recuperará totalmente su funcionalidad. En el caso de que se consideren los nodos que no llegan a recuperarse, por ejemplo, por agotamiento total de sus baterías, habrá que contemplar el uso del parámetro ν que representa la tasa de nodos caídos.

Para comenzar, con el desarrollo del modelo epidémico SIR determinista de propagación de ataques *jamming*, se toman como referencia las ecuaciones del modelo

SIR determinista clásico descritas en el Capítulo 4. Se puede asumir que el tiempo medio de duración del ataque es suficientemente pequeño como para que no se tengan en cuenta aspectos como el fallo de los nodos por causas naturales, así como la adición de nuevos nodos en la red, por lo que la población total de los nodos N se supone constante. Esta población quedará definida, por tanto, por los grupos de individuo $S(t)$, $I(t)$, $R(t)$ y $D(t)$, que corresponden respectivamente a los nodos *Susceptibles*, *Inalcanzables*, *Recuperados* y *Caidos (Dropped)*, con $N = S(t) + I(t) + R(t) + D(t)$, teniendo en cuenta, además, que este modelo solo tiene sentido siempre y cuando el número de nodos de cada grupo permanezcan en valores positivos. El modelo propuesto se describe, por tanto, mediante el siguiente sistema de ecuaciones diferenciales ordinarias:

$$\frac{dS(t)}{dt} = -\beta S(t)I(t) \quad 5.1$$

$$\frac{dI(t)}{dt} = \beta S(t)I(t) - (\gamma + \nu)I(t) \quad 5.2$$

$$\frac{dR(t)}{dt} = \gamma I(t) \quad 5.3$$

$$\frac{dD(t)}{dt} = \nu I(t) \quad 5.4$$

$$\frac{dC(t)}{dt} = \beta S(t)I(t) \quad 5.5$$

con $\beta = k \cdot \lambda$, $\nu = X/t_D$ y $\gamma = (1-X)/t_R$. La ecuación $dC(t)/dt$ permite obtener además el número acumulado de nodos afectados por el ataque.

Como ya se comentó anteriormente, un enfoque matemático típico para el estudio de la dinámica de propagación un brote epidémico, consiste analizar la estabilidad local de los puntos de equilibrio del sistema de ecuaciones diferenciales que lo componen. La propiedad principal de estos puntos es que, si se produce una ligera perturbación en el sistema, y éste se desplaza a algún punto cercano al punto estacionario, entonces el sistema debería volver a este punto estacionario [125]. Desde el punto de vista epidemiológico, los dos puntos de equilibrio de interés son el libre de enfermedad (DFE) y el endémico (EE) siendo el número reproductivo básico el valor umbral que los distingue, dado por $\mathcal{R}_0 = \beta/(\gamma+\nu)$.

Para el caso del modelo de propagación de ataques *jamming* propuesto, los puntos de equilibrio reflejarán, por un lado, la situación en la que el ataque no se propaga por la red (*Attack Free Equilibrium*, AFE) representando, por tanto, un

escenario en el que el ataque es prácticamente imperceptible por los nodos, no causando efectos negativos en el normal funcionamiento de la red. De forma análoga, el escenario equivalente al Equilibrio Endémico (*Endemic Attack*, EA), vendrá dado por una situación en la que el ataque *jamming* persiste de forma continuada, afectando a un gran número de nodos y provocando la caída de la red. Es fácil de comprobar que la situación deseada en la red de sensores inalámbrica, corresponde con una situación en la que, en ausencia de nodo *jammer* alguno, el conjunto de nodos sensores se encuentre en un equilibrio dado por una población constante de nodos susceptibles, siendo dicho punto de equilibrio de la forma $\{S, I, R, D\} = \{S_0, 0, 0, 0\}$, asumiendo que $N \approx S_0$.

Con el fin de determinar los efectos del ataque al final del período de estudio, también se adoptarán las ecuaciones del modelo SIR determinista que permitan obtener una relación entre el número reproductivo básico \mathcal{R}_0 , y el tamaño final del ataque. Estas ecuaciones se obtenían en función del número inicial de nodos susceptibles S_0 , y del número final de nodos que escaparon del ataque S_∞ .

$$\mathcal{R}_0 = \frac{\ln S_0 - \ln S_\infty}{1 - S_\infty/S_0} \quad 5.6$$

Con este conjunto de ecuaciones, queda completado el modelo SIR determinista que se utilizará posteriormente para elaborar el estudio simulado.

5.7 Modelos *fenomenológicos* para el estudio de la propagación de ataques *jamming*

El objetivo buscado con la aplicación de los modelos basados en la Teoría del Crecimiento de la Población es aportar un enfoque alternativo para la caracterización y análisis de la propagación de ataques *jamming*, especialmente cuando sólo se dispone de datos empíricos relativos al número de nodos afectados por el ataque. En este sentido, para la aplicación de estos modelos se precisa conocer la incidencia o número de nodos afectados para cada instante t . Los parámetros obtenidos tras la resolución de estos modelos permitirán, además de representar las curvas de propagación y aportar información relativa a la incidencia del ataque dentro de la población de nodos, realizar predicciones a corto y medio plazo de la dinámica de propagación del ataque.

5.7.1 Modelo de Crecimiento Generalizado (GGM)

Para la aplicación del Modelo de Crecimiento Generalizado (*Generalized Growth Model*, GGM), se asume una dinámica de crecimiento sub-exponencial al comienzo del ataque y se define mediante la ecuación diferencial:

$$\frac{dC(t)}{dt} = C'(t) = rC^p(t) \quad 5.18$$

donde $C'(t)$ representa la incidencia o número de nodos inalcanzables o afectados para cada instante t , mientras que la solución $C(t)$ es el número acumulado de nodos inalcanzables en el tiempo t . Para una población de N nodos $C'(t) = N - A(t)$. El parámetro r denota la tasa de crecimiento intrínseca ($1/t$), y el parámetro p es la *desaceleración del factor de crecimiento* donde $p \in [0, 1]$. La solución a esta ecuación diferencial viene dada por la siguiente fórmula:

$$C(t) = \left(\frac{r}{n}t + \sqrt[n]{C_0} \right) \quad 5.19$$

donde, n es un número entero positivo, $p = 1 - 1/n$ y C_0 representa el número de casos en el momento en que el comienza análisis del ataque. Si $p = 0$, esta ecuación diferencial describe una curva de incidencia constante en el tiempo, donde el número acumulado de casos crece linealmente; si $p = 1$, se obtiene un modelo de dinámica de crecimiento exponencial, siendo la solución de la ecuación $C(t) = C_0 e^{rt}$ es donde C_0 es el número inicial de casos. Si se obtienen valores intermedios de p entre 0 y 1, la ecuación 5.18 describe un comportamiento de crecimiento sub-exponencial. Este modelo, puede contemplar, además, un crecimiento más rápido que exponencial, es decir, para $p > 1$ pueden darse casos de un crecimiento súper-exponencial [128].

5.7.2 Modelo Generalizado de Crecimiento Logístico (GLGM)

Si bien con la aplicación del modelo GGM se puede obtener una aproximación adecuada durante la fase inicial de la dinámica de propagación del ataque, este modelo no tiene en cuenta las reducciones en la incidencia debido a la inmunidad de los nodos o a la implementación de protocolos capaces de sortear al nodo atacante, por lo que se

obtendría un crecimiento ilimitado en el número de nodos afectados. Para resolver este problema, se aplica el modelo de crecimiento logístico generalizado (*Generalized Logistic Growth Model*, GLGM) el cual aporta un nivel de saturación que representa un límite superior para el crecimiento del ataque. Este límite, la capacidad de carga K , representa en este modelo el tamaño final del ataque, esto es, el número de nodos afectados tras el ataque *jamming*. Para la aplicación del modelo de crecimiento logístico generalizado (GLGM) se utiliza la ecuación 4.20

$$C'(t) = rC^p(t) \left(1 - \frac{C(t)}{K}\right) \quad 5.20$$

donde $C'(t)$ representa la incidencia o número de nodos inalcanzables o afectados para cada instante t , mientras que la solución $C(t)$ es el número acumulado de nodos inalcanzables en el tiempo t . El parámetro r denota la tasa de crecimiento intrínseca ($1/t$), y el parámetro p es la *desaceleración del factor de crecimiento* donde $p \in [0, 1]$. Este modelo, también se puede considerar un crecimiento súper-exponencial, con $p > 1$ [128]. El parámetro $K > 0$ representa el tamaño final del ataque, en número total de nodos afectados. Este parámetro es crucial para generar pronósticos tras el pico del ataque y, además, puede vincularse al número reproductivo básico \mathcal{R}_0 . En efecto, al final del ataque, la ecuación 5.6 del modelo SIR determinista permite obtener una relación entre el número reproductivo básico y el tamaño final del ataque, en función de la población inicial de nodos N , del número inicial de nodos susceptibles S_0 , y del número final de nodos que escaparon del ataque S_∞ . Asumiendo que al inicio del ataque se tiene $N \approx S_0$, y que $K = S_0 - S_\infty$, entonces la ecuación 5.6 puede reescribirse en función de S_0 y K :

$$\mathcal{R}_0 = \frac{S_0(\ln S_0 - \ln S_\infty)}{K} = \frac{S_0(\ln S_0 - \ln (S_0 - K))}{K} \quad 5.21$$

Recordar que, para una población constante de N nodos, se define $A(t)$ como el número de nodos alcanzados por el coordinador en cada instante t , y por lo tanto se tendrá que $C'(t) = N - A(t)$.

5.8 Métodos de estimación y ajuste de parámetros

El objetivo principal del modelado matemático propuesto es caracterizar la dinámica de propagación del ataque *jamming*, partiendo del conjunto de datos empíricos u observaciones proporcionadas por [22]. Para ello, se han de determinar los parámetros que proporcionan el mejor ajuste del modelo con respecto al conjunto de datos, proporcionados para cada uno de los casos de ataque y escenarios propuestos. Como parte del proceso de estimación de los parámetros, se contempla también la cuantificación del intervalo de confianza de dichos parámetros.

En este estudio, se ha seguido un proceso que comienza con el ajuste inicial de los parámetros partiendo del conjunto de datos de referencia, aplicando el método de ajuste de mínimos cuadrados no lineal. Dado que las estimaciones de parámetros para un sistema dinámico dado suelen estar sujetas a ciertas fuentes de incertidumbre (dispersión temporal de los datos de referencia, supuestos empleados para inferir las estimaciones del modelo, o los algoritmos empleados, entre otros), es preciso cuantificar dicha incertidumbre. Esta cuantificación, se ha realizado mediante el reajuste de los parámetros inicialmente estimados mediante la generación de un subconjunto de m series temporales de datos basadas en una distribución de error conocida y aplicando nuevamente el método de ajuste de mínimos cuadrados no lineal. En este estudio, se ha cuantificado la incertidumbre de los parámetros, que surge de la dispersión temporal o ruido en los datos de referencia. Finalmente, utilizando el conjunto de parámetros obtenidos de las m reestimaciones, se procede a construir distribución de probabilidad correspondiente a éstos, y a construir sus intervalos de confianza.

5.8.1 Ajuste de parámetros

Una de las aproximaciones utilizadas para estimar los parámetros a partir de datos empíricos u observaciones es aplicar un algoritmo de ajuste por mínimos cuadrados no lineal. Este método intenta obtener una función $y = f(t, \Phi)$, que representa la solución de la curva del modelo deseado con respecto al tiempo, que mejor se ajusta a un conjunto de datos dado. Para este trabajo se ha utilizado la función específica implementada en MATLAB que resuelve el método de mínimos cuadrados no lineal, mediante el uso tanto del algoritmo *Trust-Region-Reflective*, como el

algoritmo *Levenberg-Marquardt* [145], [146], [147]. La solución obtenida proporciona el parámetro o coeficiente Φ , que minimizan la suma del cuadrado de las diferencias entre el modelo deseado y el conjunto de datos de referencia. Básicamente, estos métodos consideran un conjunto de parámetros $\Phi = (\Phi_1, \Phi_2, \dots, \Phi_k)$, una familia de curvas $y = f(t, \Phi)$, que dependen de los parámetros Φ , y un conjunto temporal de datos de referencia $(t_1, y_1), (t_2, y_2), \dots, (t_n, y_n)$. El ajuste por mínimos cuadrados no lineal, intenta encontrar el valor del conjunto de parámetros $\hat{\Phi} = (\hat{\Phi}_1, \hat{\Phi}_2, \dots, \hat{\Phi}_k)$ tal que la curva $y = f(t, \hat{\Phi})$ minimiza la función objetivo:

$$\hat{\Phi} = \min_{\Phi} \|f(t_i, \Phi) - y_{t_i}\|^2 = \min_{\Phi} \sum_{t=1}^n (f(t_i, \Phi) - y_{t_i})^2 \quad 5.22$$

Para utilizar la función de ajuste por mínimos cuadrados correctamente, deben definirse para cada uno de los parámetros deseados θ , los límites superior e inferior, y un valor inicial. Además, una vez estimados los parámetros, la función proporciona los residuos, como la diferencia entre el mejor ajuste del modelo y los datos de la serie temporal en función del tiempo, en la forma $res(t_i) = f(t_i, \hat{\Phi}) - y_{t_i}$, pudiéndose utilizar para evaluar la calidad del ajuste del modelo. De forma general, un patrón aleatorio en la variación temporal de los residuos sugiere un buen ajuste del modelo a los datos. En cambio, las desviaciones sistemáticas del modelo con respecto a los datos (como una correlación temporal) indican que el modelo se desvía sistemáticamente. Si además el modelo se utiliza para realizar pronósticos, es particularmente importante que los residuos no estén correlacionados y que la varianza de éstos sea aproximadamente constante [148].

Una vez obtenida esta estimación de los parámetros $\hat{\Phi}$, ya se dispone de una primera aproximación de las curvas $y = f(t, \hat{\Phi})$, como solución del modelo deseado.

5.8.2 Cuantificación de los intervalos de confianza de los parámetros

Como se indicó anteriormente, las estimaciones de parámetros para un sistema dinámico dado suelen estar sujetas a ciertas fuentes de incertidumbre, por lo que es necesario cuantificar la incertidumbre de las estimaciones de estos parámetros. En este caso, se han establecido como referencia el 95% para construir los intervalos de confianza, e identificar así la desviación potencial de cada parámetro. Uno de los métodos para cuantificar la incertidumbre es el *bootstrapping* paramétrico [131], [148],

[149], [150]. Básicamente, este método realiza una reestimación de los parámetros $\hat{\Phi}$ obtenidos anteriormente como mejor ajuste del modelo. Para ello se realiza un muestreo de forma repetitiva de los puntos de la curva de ajuste del modelo $y = f(t, \hat{\Phi})$, generando múltiples observaciones $y_i = f(t, \hat{\Phi}_i)$, de datos sintéticos. Para este estudio se ha realizado un *bootstrapping* paramétrico de $m = 300$ observaciones, asumiendo, además, que la serie temporal de datos sigue una estructura de error de distribución de *Poisson*, centrada en la media de los puntos temporales de cada observación. Esto genera un nuevo conjunto de curvas dadas como solución del modelo, $y_1 = f_1(t, \hat{\Phi}_1)$, $y_2 = f_2(t, \hat{\Phi}_2)$, ..., $y_m = f_m(t, \hat{\Phi}_m)$, así como el conjunto de parámetros reestimados $\hat{\theta}_i$, donde $i = 1, 2, \dots, m$.

Una vez que los parámetros del modelo han sido reestimados mediante la técnica de *bootstrapping*, entonces es posible caracterizar las distribuciones empíricas obtenidas y construir los intervalos de confianza. La incertidumbre resultante en torno al nuevo ajuste del modelo viene dada por el conjunto de curvas $y_i = f(t, \hat{\Phi}_i)$, y por los parámetros asociados. Para determinar intervalo de confianza del 95% de los parámetros estimados, se ha utilizado la función *cuantil*. En este caso, se calcula el *cuantil* 0.95 asociado a la función de distribución de los parámetros reestimados $\hat{\Phi}_i$, tomados como una variable aleatoria. La función utilizada corresponde al paquete MCMCSTAT [151] el cual contiene un conjunto de funciones de MATLAB para el análisis estadístico de modelos matemáticos mediante el uso de simulaciones de Monte Carlo utilizando Cadenas de *Markov* [152].

Toda la programación de las funciones indicadas se ha desarrollado en MATLAB, obteniendo para cada parámetro $\hat{\Phi}$ un vector $[a \ b \ c]$ donde a es la media μ del valor estimado para el parámetro $\hat{\Phi}_i$, mientras que a y b representan, respectivamente, el límite inferior y superior del 95% del intervalo de confianza, centrado en la media $\mu = \sum_{i=1}^m \hat{\Phi}_i / m$. Esta cuantificación permite identificar la precisión con la que el parámetro ha sido estimado, donde un rango finito de valores indica que el parámetro ha sido estimado con precisión, mientras que un rango más amplio podría ser indicativo de una falta de precisión en la estimación.

5.9 Conclusiones

En el presente Capítulo se han presentado los materiales y métodos utilizados para el desarrollo de la tesis. En este sentido, se ha descrito, en primer lugar, el conjunto de datos que se utilizará para la validación de los modelos epidemiológicos propuestos. Por otra parte, se han descrito los modelos epidemiológicos que se utilizarán para análisis simulado de la propagación de ataques *jamming* objeto de esta tesis. Dentro de los diferentes modelos, se ha prestado especial atención a la importancia del conocimiento de los parámetros que lo definen. Por ejemplo, el número reproductivo básico \mathcal{R}_0 del modelo SIR, que marcará la diferencia entre un proceso epidémico, que propagará el ataque a través de la red, o un proceso no epidémico, en el que ataque se extinguirá con rapidez; la tasa de contagio β , que puede utilizarse como un indicativo de la severidad del ataque, el parámetro $1/\gamma$, que permitirá conocer la persistencia del ataque, y el parámetro $1/\mu$ con la inclusión, de un grupo para contabilizar los posibles nodos que pierdan totalmente su funcionalidad durante el ataque, lo que dota al modelo de una mayor aplicabilidad. También se ha puesto énfasis en formular el modelo incluyendo la estructura de la red sobre la que se propaga el ataque *jamming*, para lo que se ha descompuesto la tasa de contagio en dos parámetros, donde uno de ellos representa la tasa promedio de contactos entre nodos susceptibles y afectados, estando estrechamente relacionado con los enlaces radio entre nodos.

Finalmente, se han propuesto modelos alternativos a los modelos mecánicos clásicos, describiendo los modelos de crecimiento generalizado y crecimiento logístico. En este caso, los parámetros que definen estos modelos están representados por denota la tasa de crecimiento intrínseca r , la desaceleración del factor de crecimiento p , y el tamaño final del ataque K .

Por último, se han descrito los métodos usados para la estimación de los parámetros de caracterización de los ataques, y de sus correspondientes intervalos de confianza.

Con estos elementos, se está en disposición de realizar la validación de los modelos epidemiológicos propuestos mediante un estudio experimental, y como contribución principal de esta investigación.

CAPÍTULO

6

**Estudio epidemiológico de la propagación
de ataques *jamming***

En este Capítulo, y como contribución principal de esta investigación, se ha realizado la validación experimental de los modelos propuestos para el desarrollo de esta Tesis, mediante la elaboración de un estudio epidemiológico donde, a través de un conjunto de simulaciones, se caracterizan y analizan los ciberataques *jamming* de tipo aleatorio y reactivo, llevados a cabo contra una red de sensores inalámbricos. Junto con los materiales y métodos descritos en el Capítulo anterior, los modelos empleados a lo largo de este estudio epidemiológico son el modelo SIR determinista, al que se le añade el grupo de los nodos caídos, y los modelos de crecimiento generalizado (GGM) y de crecimiento logístico generalizado (GLGM) respectivamente.

En ambos casos, se sigue un procedimiento de dos fases donde, en primer lugar, se realiza una estimación inicial de los parámetros que caracterizan el modelo aplicado, mediante el método de ajuste de mínimos cuadrados no lineal. Posteriormente, con los datos obtenidos se realiza una segunda reestimación de dichos parámetros, asumiendo que la serie temporal de estos datos sigue una estructura de error de distribución de *Poisson*. Como resultado, se obtienen un conjunto de curvas características que representan el mejor ajuste de la dinámica de propagación del ciberataque junto con los resultados de la incertidumbre asociada. Para cada experimento, los valores obtenidos se han cotejado con los datos proporcionados en [22] como se describió en el Capítulo 5.

6.1 Introducción

Para llevar a cabo este estudio epidemiológico experimental sobre la propagación de ataques *jamming*, se ha desarrollado un programa en MATLAB para cada uno de los modelos propuestos, con el que se obtienen las curvas epidémicas, junto con los parámetros que caracterizan a cada uno de los casos de ataque *jamming*. El programa realiza principalmente dos funciones. En primer lugar, obtiene una estimación de los parámetros matemáticos $\hat{\Phi} = (\hat{\Phi}_1, \hat{\Phi}_2, \dots, \hat{\Phi}_k)$ que definen a cada modelo, para lo que se aplica el método ajuste de mínimos cuadrados no lineal, el cual utiliza los algoritmos *Trust-Region-Reflective* y *Levenberg-Marquardt* [145], [146]. Para obtener esta estimación inicial de los parámetros, se han tomado como referencia las series de datos $y_t = y_1, y_2, \dots, y_n$, proporcionados en [22]. En adelante, estos datos serán mencionados como los *datos de referencia*. Con los valores de estos parámetros se obtienen una primera aproximación de las curvas epidemiológicas características de cada ataque $y = f(t, \hat{\Phi})$, mediante la resolución de las diferentes ecuaciones diferenciales o sistemas de ecuaciones diferenciales, según el modelo aplicado para cada caso. Cabe señalar que la función de ajuste por mínimos cuadrados no lineal es bastante sensible a la definición inicial de los valores esperados de los parámetros y, por lo tanto, se ha tomado como referencia inicial los valores obtenidos en sendos trabajos publicados como parte del desarrollo de esta Tesis [20], [21]. A su vez, también se han realizado diversos experimentos previos para analizar la dinámica de los ataques y fijar así los umbrales de trabajo para los parámetros. Además, una vez estimados los parámetros, el programa proporciona los residuos, obtenidos como la diferencia entre el mejor ajuste del modelo y los datos, en función del tiempo.

La segunda función del programa, que se ejecuta una vez obtenido el primer ajuste de las curvas del modelo, es cuantificar del intervalo de confianza de los parámetros estimados al 95%, para identificar la desviación potencial o incertidumbre de éstos. El método utilizado para esta cuantificación es el *bootstrapping* paramétrico ya descrito en el Capítulo 5. Básicamente, en esta fase se vuelven a estimar los parámetros $\hat{\Phi} = (\hat{\Phi}_1, \hat{\Phi}_2, \dots, \hat{\Phi}_k)$ del modelo, utilizando nuevamente el método de mínimos cuadrados no lineal. Sin embargo, en esta ocasión se toman como referencia las series temporales de datos obtenidas en la fase anterior, asumiendo que sigue una estructura de error de distribución de *Poisson*, centrada en la media de los puntos de cada

observación. Para ello, se muestrean repetidamente los puntos de las curvas epidémicas (en este experimento se realizan 300 muestreos para cada curva), obteniendo múltiples observaciones y generando un nuevo conjunto de datos sintético o distribución empírica. Posteriormente, se aplica nuevamente el método de mínimos cuadrados no lineal sobre cada una de estas 300 realizaciones, obteniendo una nueva estimación de los parámetros matemáticos fundamentales que definen a cada modelo. Este algoritmo minimiza la suma de los cuadrados de las diferencias entre los datos de referencia, y los puntos de cada observación obtenidos de las 300 curvas generadas.

La figura adjunta representa un diagrama de bloques de alto nivel con las distintas funciones del programa MATLAB propuesto en este estudio epidemiológico.

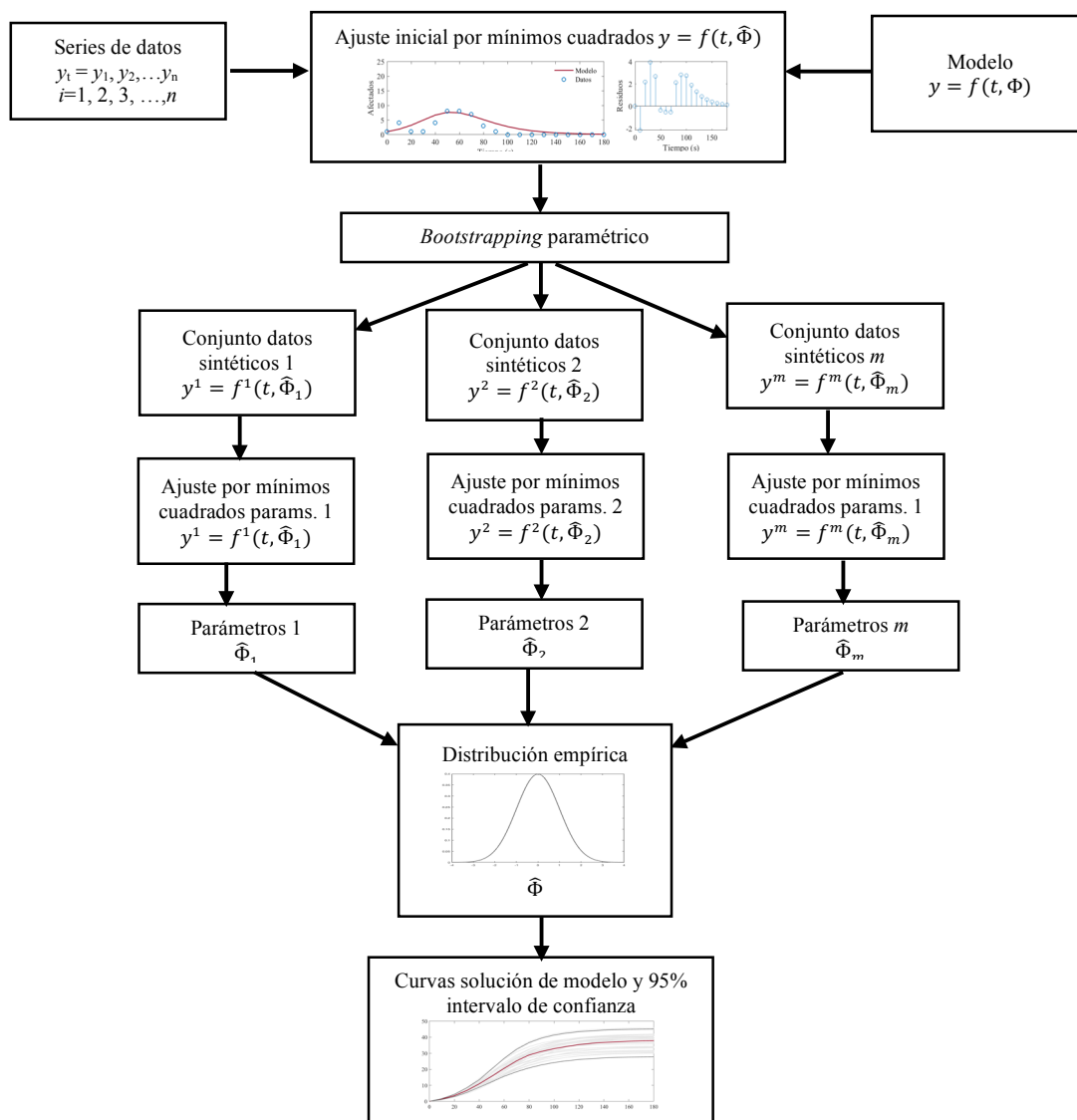


Figura 6.1. Diagrama de alto nivel de las funciones realizadas por el programa MATLAB.

El intervalo de confianza al 95% para el conjunto de parámetros se obtiene, tal y como se indicó en el Capítulo 5, aplicando la función de cálculo de *cuantiles*, correspondiente al paquete MCMCSTAT que contiene un conjunto de funciones de MATLAB para análisis estadísticos de modelos matemáticos [151], [152].

Finalmente, para obtener una visión del ajuste proporcionado por el modelo, se grafican en una misma figura, las soluciones de las ecuaciones diferenciales experimentales obtenidas para cada uno de los ataques *jamming* según el modelo aplicado, junto con los datos de referencia. Esto permite obtener una comparativa de las correspondientes curvas epidémicas obtenidas por el modelo propuesto con respecto a los datos de referencia.

6.2 Aplicación del modelo epidémico SIR determinista para la caracterización y análisis de la propagación de ataques *jamming*

Para llevar a cabo este experimento se ha utilizado una extensión del modelo SIR determinista (Susceptibles, Inalcanzables, Recuperados y Caídos) tal y como se ha descrito en el Capítulo 5. Este modelo queda definido por el conjunto de ecuaciones diferenciales $dS(t)/dt$, $dI(t)/dt$, $dR(t)/dt$ y $dD(t)/dt$. En este caso, los parámetros principales para la caracterización del ataque son la tasa de contagio β , la tasa de recuperación γ , y la tasa de nodos caídos ν , para cada uno de los 27 casos de ataque *jamming* a estudio.

En primer lugar, se han obtenido las curvas características del ataque mediante el ajuste de los parámetros β , γ , ν , en base a los datos de referencia. Posteriormente, se han construido los intervalos de confianza al 95 % de dichos parámetros, cuantificando la incertidumbre de éstos. La calibración previa del modelo y la posterior obtención de los intervalos de confianza resultantes proporcionan un reajuste de los parámetros, obteniendo el conjunto de curvas solución del sistema de ecuaciones diferenciales $dS(t)/dt$, $dI(t)/dt$, $dR(t)/dt$ y $dD(t)/dt$, que representan cómo la población de nodos se mueve de un compartimento a lo largo del tiempo.

Dado que la función de ajuste por mínimos cuadrados no lineal requiere la definición inicial de los valores esperados de los parámetros, en la Tabla 6.1 se presentan los valores propuestos para β , γ , y ν , basados en la experimentación previa.

Parámetro	Valor esperado	Límite inferior	Límite superior
Tasa de contagio β	0.002	0	0.2
Periodo de recuperación γ	0.02	0	0.2
Tasa de nodos caídos ν	0	0	0.002

Tabla 6.1. Límites y valores esperados inicial para los parámetros β, γ, ν .

De los diferentes análisis y datos obtenidos tras la simulación, se dispone de un conjunto de resultados significativos que caracterizan el ataque, tales como los parámetros β, γ , y ν , estimados, el número reproductivo básico \mathcal{R}_0 , el número máximo de nodos afectados, o el tiempo en el que se produce el pico del ataque, entre otros.

6.2.1 Estudio retrospectivo de la propagación de ataques *jamming* mediante el modelo epidémico SIR determinista

Los ataques de *jamming* llevados a cabo en este experimento, se basan en el conjunto de ataques propuestos en el trabajo de investigación [22]. Estos ataques se presentan en tres escenarios diferentes, y para cada escenario, se dividen en dos grupos, siendo los casos del 1 al 6 de ataques *jamming* aleatorio, mientras que los casos del 7 al 9 corresponden a ataques *jamming* reactivos, lo que proporciona un total de 27 casos de ataques *jamming* para su estudio. A modo de ejemplo, y con el fin de no extender en exceso este Capítulo, se expone en este apartado, los resultados experimentales obtenidos para el caso de estudio 10, correspondiente al primer ataque del escenario 2, donde se ejecuta un *jamming* aleatorio a 50 paquetes/segundo contra el protocolo AODV cuando el nodo atacante está en el centro de la red de sensores inalámbricos. Para el experimento de caracterización y posterior análisis del ataque, se ha tomado un periodo de simulación de 180 segundos, utilizando los datos aportados por [22]. Los resultados obtenidos de los experimentos realizados para otros de casos de ataques y escenarios se han incluido en el Apéndices II y III.

La Figura 6.2 muestra el mejor ajuste para cada una de las curvas del modelo SIR, tras 180 segundos de simulación, junto con los residuos obtenidos al aplicar el método de ajuste por mínimos cuadrados no lineal.

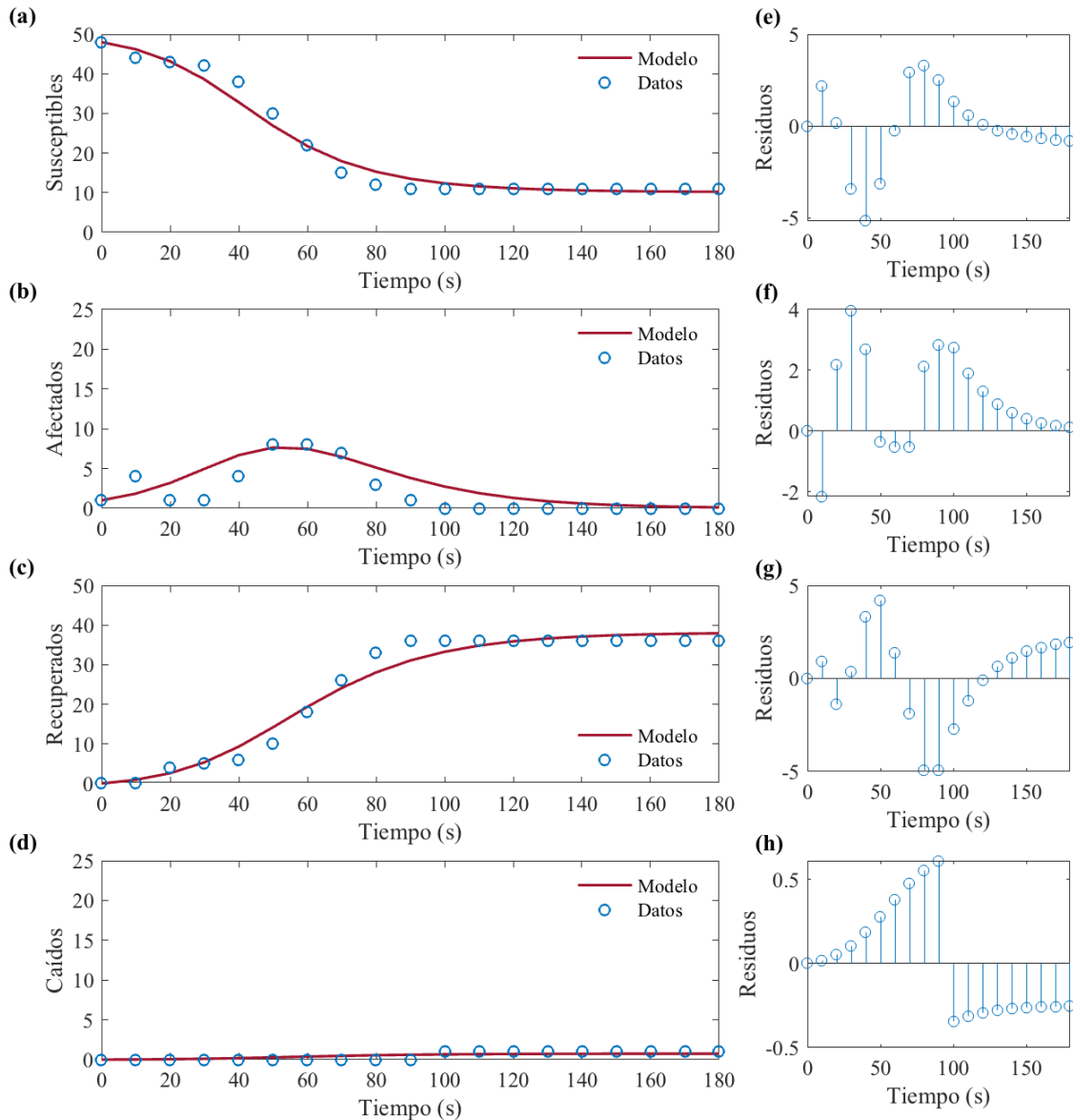


Figura 6.2. Ajuste inicial para *jamming* aleatorio a 50 paquetes/segundo contra el protocolo AODV cuando el nodo atacante está en el centro de la topología de la red.

En la Figura 6.2, las gráficas (a), (b), (c) y (d) muestran el mejor ajuste para cada una de las curvas $dS(t)/dt$, $dI(t)/dt$, $dR(t)/dt$ del modelo SIR, junto con la curva de los nodos caídos $dD(t)/dt$. Los trazos en línea roja continua representan cada una de las curvas característica del ataque para cada uno de los grupos de nodos, según el modelo propuesto para este experimento, mientras que los círculos azules representan los datos de referencia. En misma figura, las gráficas (e), (f), (g) y (h) muestra los residuos en función del tiempo. Según se observa, tanto el conjunto de curvas obtenidas en el experimento, como el patrón aleatorio de los residuos, sugiere, a priori, que el modelo ha proporcionado un ajuste razonablemente bueno para las distintas fases del ataque.

La Figura 6.3 muestra los histogramas (a), (b) y (c), con los valores correspondientes al 95% del intervalo de confianza obtenido para los parámetros β , γ , y ν , respectivamente. El histograma (d) representa el intervalo de confianza al 95%, del número reproductivo básico \mathcal{R}_0 , estimado con la Ecuación 5.6 descrita en el Capítulo 5. La obtención de los intervalos de confianza se realiza mediante la aplicación del método de *bootstrapping* ya descrito, y asumiendo una estructura de error basada en la distribución de *Poisson*.

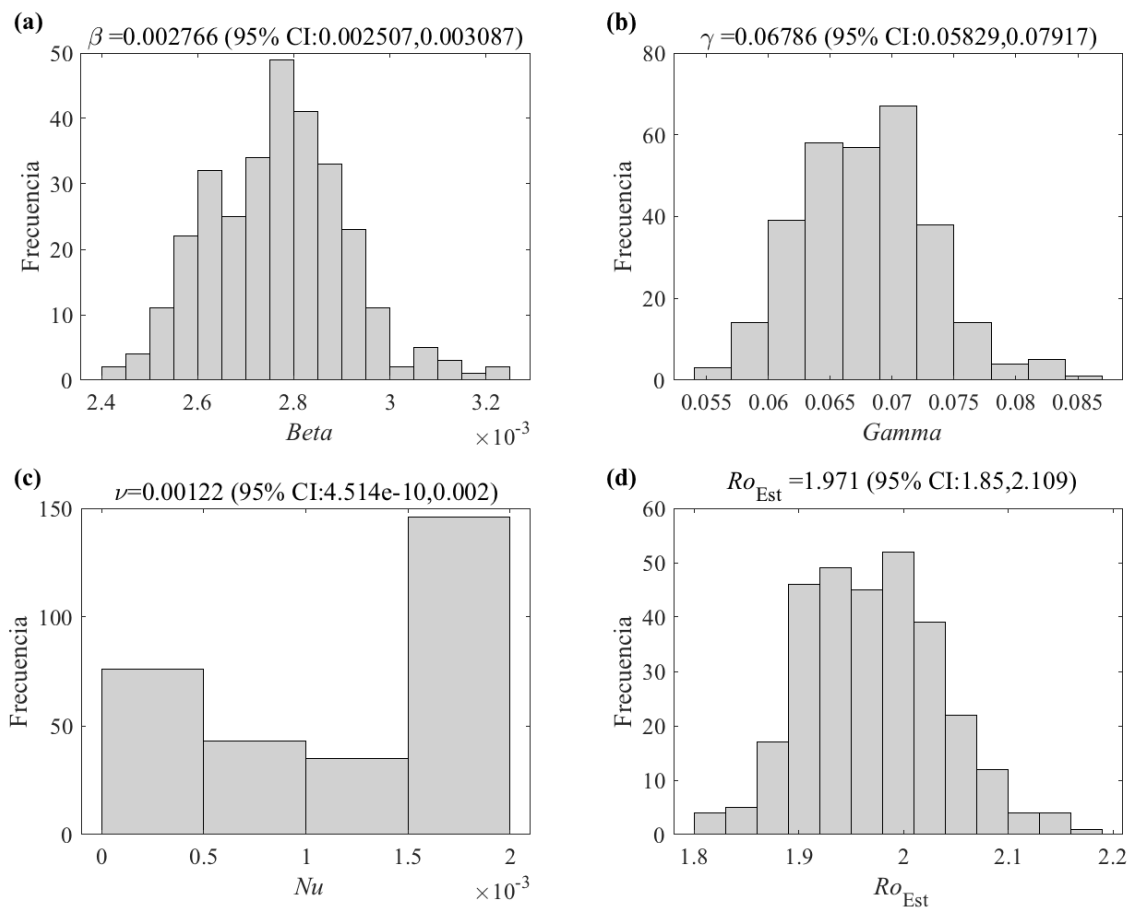


Figura 6.3. Histogramas de las distribuciones empíricas para las estimaciones del 95% de los intervalos de confianza de los parámetros β , γ , ν , y \mathcal{R}_0 .

Tal y como se indicó anteriormente, la cuantificación y obtención de los intervalos de confianza, permite identificar la precisión con la que cada uno de los parámetros ha sido estimado. En este caso, se observa un rango finito de valores alrededor de la media obtenida, lo que indica que el conjunto de parámetros ha sido estimado con una precisión aceptable. Cabe comentar, que en el caso del parámetro ν , se observa un intervalo de confianza más amplio, sin embargo, el orden de magnitud de este parámetro hace que esto no afecte al resultado obtenido.

Por otro lado, en la Figura 6.4 se han representado las curvas características del ataque tras el reajuste de los parámetros, junto con las curvas de la distribución de error generadas para la obtención del intervalo de confianza al 95% de dichos parámetros.

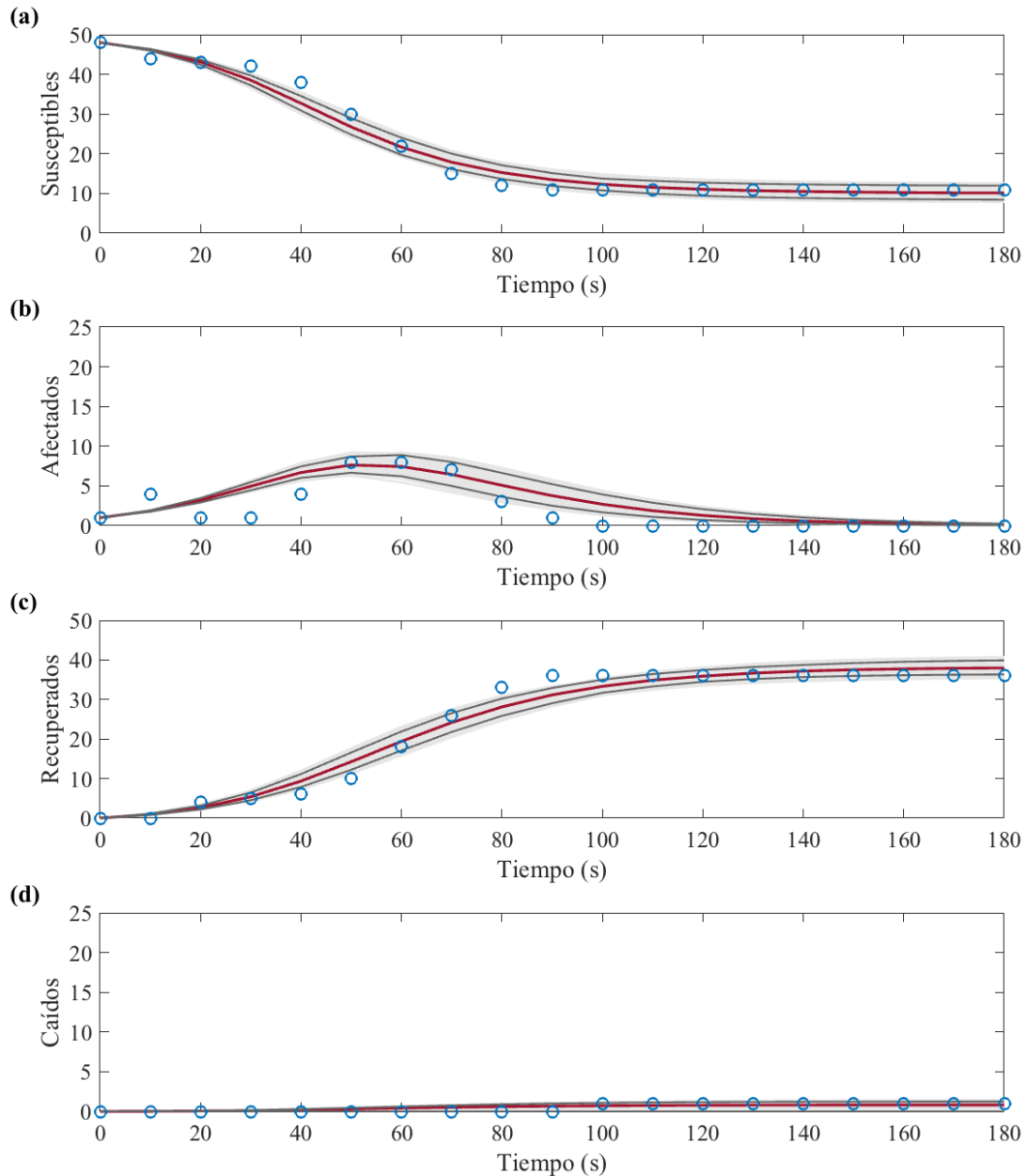


Figura 6.4. Reajuste de parámetros e intervalos de confianza obtenidos mediante *bootstrapping* para *jamming* aleatorio a 50 paquetes/segundo contra el protocolo AODV cuando el nodo atacante está en el centro de la topología de la red.

En la Figura 6.4, las gráficas (a), (b), (c) y (d) muestran el mejor ajuste para cada una de las curvas $dS(t)/dt$, $dI(t)/dt$, $dR(t)/dt$ del modelo SIR, junto con la curva de los nodos caídos $dD(t)/dt$. Los trazos en línea continua roja representan las curvas características del ataque para cada uno de los grupos de nodos, obtenidos

experimentalmente según el modelo epidemiológico SIR utilizado, mientras que los círculos en azul representan los datos de referencia. Los trazos de línea gris claro representan cada una de las 300 realizaciones o *bootstrapping* obtenidas mediante la estructura de error basada en la distribución de *Poisson*. Estas curvas permiten tanto la obtención del intervalo de confianza al 95% de los parámetros, como la identificación de la desviación potencial o incertidumbre de los parámetros tras su reajuste. El conjunto de curvas características obtenidas experimentalmente, indica que el modelo ha proporcionado un ajuste con una precisión razonablemente buena, para las distintas etapas del ataque. Esto se comprueba mediante la comparación de los datos experimentales y los datos de referencia.

Como complemento a estos resultados, en la Figura 6.5 se presenta la curva de incidencia acumulada en trazo de línea continua roja, y su intervalo de confianza al 95%, obtenida experimentalmente con el modelo SIR, junto con la incidencia acumulada obtenida de los datos de referencia, representada por el trazo de línea continua azul. En epidemiología, la incidencia acumulada representa el número total de individuos que han sido afectados por una enfermedad, y considerando que la epidemia ha finalizado, éste resulta un parámetro fundamental para conocer el tamaño del brote epidémico dentro de una población. Aplicando este mismo concepto para el estudio de los ataques *jamming*, la incidencia acumulada representa cuál ha sido el efecto del ataque lanzado contra la red de sensores al finalizar éste. En el análisis detallado posterior, se comprueba que, para el caso de estudio, casi el 80% de los nodos han sido afectados por el ataque, presentando una alta severidad.

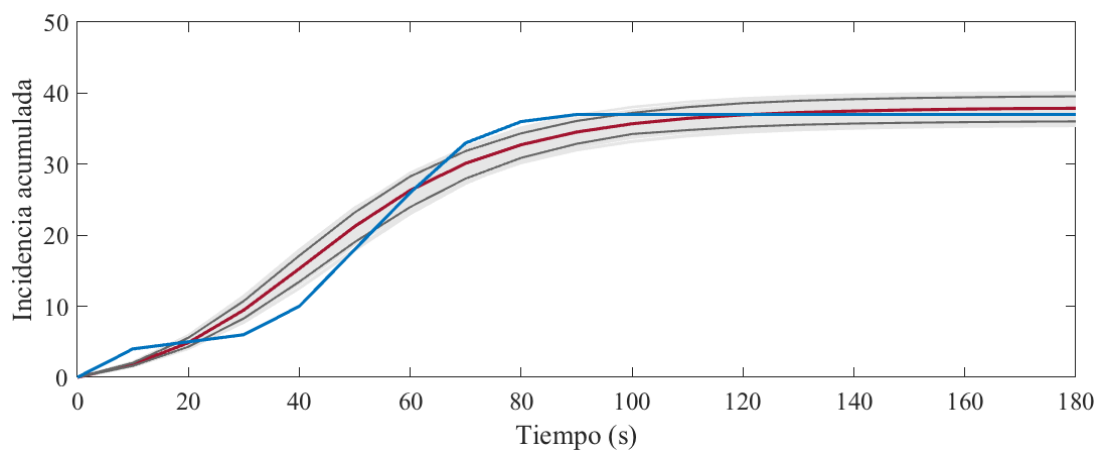


Figura 6.5. Curva de Incidencia acumulada y sus correspondientes intervalos de confianza obtenidos mediante *bootstrapping* para *jamming* aleatorio a 50 paquetes/segundo contra el protocolo AODV cuando el nodo atacante está en el centro de la topología de la red.

Finalmente, en la Figura 6.6 se presenta una comparativa de los resultados experimentales obtenidos por el modelo propuesto, con respecto a los datos de referencia, tras los 180 segundos de simulación del ataque *jamming* aleatorio a 50 paquetes/segundo cuando el nodo atacante está en el centro de la topología de red. En este caso, se ha representado en un mismo gráfico cada una de las curvas epidémicas que caracterizan el ataque como solución de las ecuaciones $dS(t)/dt$, $dI(t)/dt$, $dR(t)/dt$ y $dD(t)/dt$, obtenidas con los valores de β , γ , y ν reajustados. Los trazos de línea continua coloreada representan las curvas características del ataque para cada uno de los grupos de nodos, según el modelo epidemiológico SIR usado en el experimento, mientras que los círculos representan los datos de referencia.

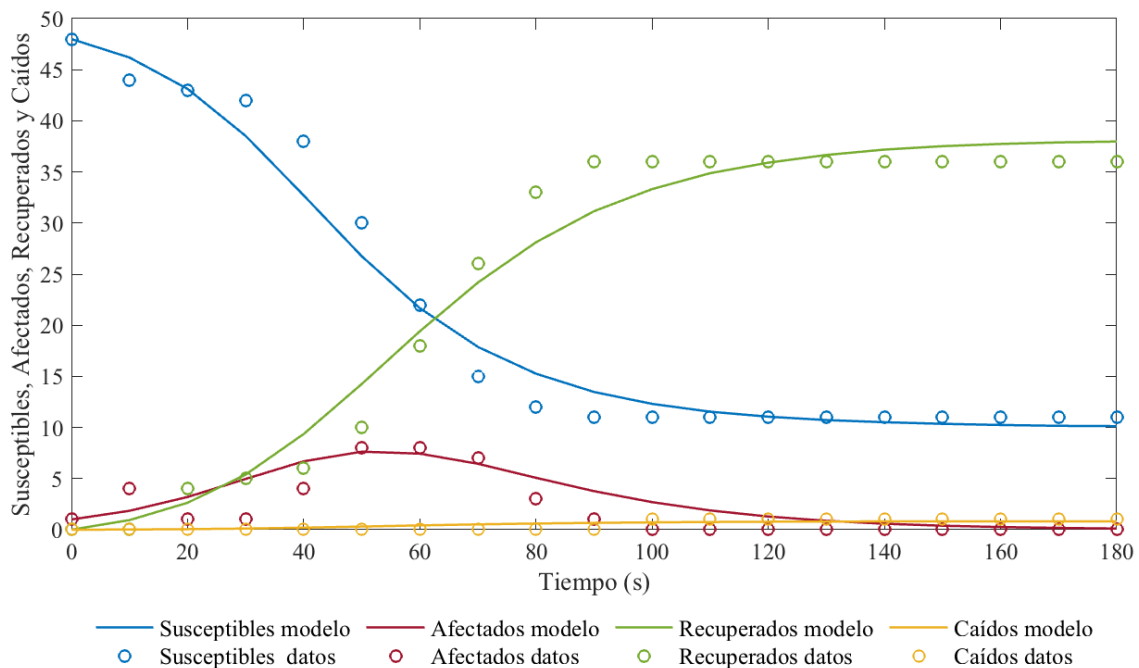


Figura 6.6. Comparativa final de los resultados experimentales obtenidos por el modelo SIR con respecto a los datos de referencia, tras los 180 segundos de simulación del ataque *jamming* aleatorio a 50 paquetes/segundo cuando el nodo atacante está en el centro de la topología de red.

En esta Figura 6.6 puede apreciarse cómo la dinámica del ataque *jamming* sigue un patrón similar al de un brote epidémico, en el que los individuos de la población afectada (en este caso los nodos) van pasando de un grupo a otro a lo largo del tiempo, según su estado frente al ataque (Susceptibles, Afectados o Inalcanzables, Recuperados y Caídos). La interpretación de esta figura es la siguiente.

En el instante inicial, $t = 0$, se introduce en la población de nodos de la red inalámbrica un nodo atacante que actuará como “*paciente cero*”. Al cabo de unos

segundos, comienzan a observarse los primeros efectos del ataque al comenzar a aumentar el número de nodos inalcanzables por el coordinador, representados en el modelo SIR por la curva $dI(t)/dt$, en trazo de línea continua roja. Se observa que este incremento de nodos afectados alcanza su pico máximo (pico epidémico) a los 50 segundos, y a partir de aquí el número de nodos afectados por el ataque comienza a descender. En este punto, el modelo ha estimado dicho máximo en 7,64 nodos afectados o inalcanzables por el coordinador mientras que, según los datos de referencia, en este punto se tienen 8 nodos inalcanzables. También se observa, tanto para el modelo como para los datos de referencia, que los primeros nodos recuperados aparecen entorno a 20 segundos después de iniciarse el ataque. Teniendo en cuenta que los intervalos de muestreo son de 10 segundos, y que en el experimento se ha estimado un tiempo de recuperación o persistencia del ataque de $1/\gamma = 14.736$ segundos, se comprueba que ambos valores están alineados, ya que los primeros nodos deberían aparecer entorno a los 24,736 segundos. Estos nodos recuperados, correspondientes en el modelo SIR a la ecuación $dR(t)/dt$, se han representado en la figura con trazo de línea continua verde claro, y con círculos del mismo color para los datos de referencia. En esta misma figura, se han representado los nodos que no han sido afectados por el ataque, esto es, que continúan como susceptibles dentro de la población, representados en el modelo SIR por la ecuación $dS(t)/dt$. Estos nodos se han graficado en la figura con trazo de línea continua azul claro para el modelo, y con círculos del mismo color para los datos de referencia. Cabe indicar que, según dichos datos, al final de los 100 segundos de ataque el nodo coordinador sólo es capaz de alcanzar a 47 nodos, de los 48 que inicialmente componían la red. Esta circunstancia se ha interpretado como la existencia de un nodo caído. Por lo tanto, el modelo ha sido capaz de detectar en esta situación en la fase final del ataque, tal y como puede verse en la existencia de valores distintos de cero en el grupo de los nodos caídos dados por la ecuación por la ecuación $dD(t)/dt$, representados en la figura por el trazo de línea continua naranja claro y círculos del mismo color.

Finalmente, para obtener una aproximación de la severidad del ataque se puede analizar el número de nodos susceptibles final S_∞ , y la incidencia acumulada C_∞ , pues ambos valores proporcionan la dimensión o tamaño final de la epidemia. En el primer caso, el experimento arroja un valor para S_∞ de 10.13 nodos, mientras que los datos de referencia dan un valor de 11 nodos. Desde el punto de vista del modelo epidémico, esto indica que de un total de 48 nodos susceptibles que componían población de nodos al

inicio de ataque, sólo 10 han salido indemnes de éste. Como consecuencia, el ciberataque ha afectado a casi el 80% de la población. Análogamente, como ya se adelantó anteriormente, la incidencia acumulada C_{∞} , también proporciona una estimación de la severidad del ataque, para la que el modelo estima un valor de 37.87 nodos afectados, mientras que los datos de referencia indican un valor de 37 nodos. Aquí, también se comprueba que de los 48 nodos que componían población al inicio de ataque, casi el 80% han sido afectados por el ataque, corroborando lo obtenido para S_{∞} .

Por otro lado, como se indicó anteriormente, el número reproductivo básico es otro parámetro que puede utilizarse para analizar el impacto que una epidemia causada por un determinado patógeno ha tenido en una población concreta. En este ejemplo, es posible realizar su cálculo una vez que se dispone de los parámetros β , γ , y ν , y de los valores de S_0 y S_{∞} . Para la obtención del \mathcal{R}_0 estimado tanto del modelo como de los datos de referencia, se ha utilizado la Ecuación 5.6, descrita en el Capítulo 5, donde intervienen los valores de S_0 y S_{∞} . Mientras que, para obtener un valor teórico, se ha utilizado la fórmula $\mathcal{R}_0 = \beta S_0 / (\gamma + \nu)$. Cabe señalar que, en los modelos epidémicos de tipo determinista, el número reproductivo básico se estima generalmente de forma retrospectiva, a partir de la serie de datos epidemiológicos proporcionados tras la epidemia. Para el ejemplo analizado en esta sección, los cálculos tras el experimento proporcionan un valor teórico $\mathcal{R}_0 = 1.927$ (95% CI: 1.805, 2.069), mientras que el valor estimado del modelo es $\mathcal{R}_0 = 1.971$ (95% CI: 1.850, 2.101), siendo el calculado según los datos de referencia $\mathcal{R}_0 = 1.911$. La Tabla 6.2 muestra los parámetros principales.

Parámetro	Valor experimento
Tasa de contagio β	0.002766 (95% CI: 0.002507, 0.0030869)
Periodo de recuperación γ	0.06786 (95% CI: 0.058294, 0.0791711)
Tasa de nodos caídos ν	0.001219 (95% CI: 4.514E-10, 0.002)
Tiempo de recuperación $1/\gamma$ (s)	14.7297 (95% CI: 12.65773, 17.5359)
\mathcal{R}_0 teórico modelo SIR	1.926616 (95% CI: 1.804902, 2.068928)
\mathcal{R}_0 estimado modelo SIR	1.97114 (95% CI: 1.85002, 2.109139)

Tabla 6.2. Parámetros caracterizadores del ataque *jamming* aleatorio a 50 paquetes/segundo contra el protocolo AODV cuando el nodo atacante está en el centro de la topología de la red.

Adicionalmente a los parámetros del ataque proporcionados por el modelo SIR, la Tabla 6.3 presenta una comparativa con datos extraídos experimentalmente de la simulación realizada, junto con los valores de referencia correspondientes.

Parámetro	Valor experimento	Valor datos de referencia
Pico máximo de nodos inalcanzables	7.6337	8
Tiempo del pico de ataque (s)	50	50
Incidencia acumulada de nodos	37.867	37
Nodos Susceptibles al final del ataque	10.13	11
Nodos Caídos al final del ataque	≈ 1 (0.8238)	1

Tabla 6.3. Comparativa de datos del ataque *jamming* aleatorio a 50 paquetes/segundo contra el protocolo AODV cuando el nodo atacante está en el centro de la topología de la red.

Al igual que con el resto de resultados obtenidos experimentalmente mediante el estudio simulado, en esta tabla se puede comprobar la validez del modelo SIR propuesto para la caracterización de ataques *jamming*, pues dichos resultados se ajustan a los datos de referencia aportados en [22].

La caracterización epidémica de la propagación de los ataques *jamming*, permite buscar una similitud entre la incidencia del ataque estudiado y la de algún brote epidémico conocido, mediante, por ejemplo, la comparación de sus \mathcal{R}_0 . Si bien éste se obtiene principalmente de parámetros como la duración del contagio, la probabilidad de infección y la tasa de contacto, su valor puede diferir en una misma enfermedad por diferentes factores. Además del propio método de cálculo usado para su obtención, factores ambientales, geográficas, o medidas preventivas como la vacunación, entre otros, pueden dificultar su cálculo. En el caso del ataque estudiado, se ha obtenido experimentalmente un \mathcal{R}_0 medio de 1.971, y un intervalo de confianza al 95% de 1.850 a 2.109. Este rango de valores se han encontrado algunos brotes epidémicos destacables, como, por ejemplo, la pandemia cepa de gripe A/H1N1 de 2009 en Nueva Zelanda, con un \mathcal{R}_0 medio de 1.96 e intervalo de confianza al 95% de 1.80 a 2.15 [153], [154]. También se pueden encontrar valores parecidos de \mathcal{R}_0 para la primera ola de la pandemia de Gripe Española de 1918 a 1919, donde un estudio ampliamente citado estimó un \mathcal{R}_0 medio de aproximadamente 2.0 [155].

6.2.2 Estudio predictivo de la propagación de ataques *jamming* mediante el modelo epidémico SIR determinista

Como complemento al estudio experimental de la propagación del ataque *jamming* presentada en el apartado anterior, se ha realizado un segundo experimento con el modelo SIR determinista en el que se pronostica la evolución del ataque en base a los datos de referencia obtenidos en la fase temprana del ataque. Tal y como se indicó en el Capítulo 4, los modelos deterministas como el SIR se utilizan mayoritariamente para realizar estudios epidémicos de forma retrospectiva o a posteriori, esto es, una vez que la epidemia se da por concluida y se dispone de una serie de datos conocida, al menos en un intervalo de tiempo razonablemente amplio. Sin embargo, estos modelos también pueden utilizarse, con ciertas restricciones, para realizar un estudio predictivo de la evolución de una determinada epidemia.

Para llevar a cabo este experimento, la estimación inicial de los parámetros β , γ , y ν , se realiza teniendo en cuenta sólo los datos proporcionados en los 50 segundos iniciales del ataque. El resto del proceso de cálculo, sigue los mismos pasos a descritos anteriormente, esto es, método de ajuste de mínimos cuadrados no lineal para cálculo inicial de los parámetros, y método de *bootstrapping* para cuantificar el intervalo de confianza de los parámetros al 95%. Una vez obtenida la estimación de los parámetros en la fase inicial del ataque, y cuantificada su incertidumbre, se construye un pronóstico a corto plazo mediante la propagación de dicha incertidumbre en un horizonte de T unidades de tiempo hacia adelante. En cualquier caso, este proceso de predicción de las curvas características del ataque se describe con mayor detalle en la siguiente sección, cuando se traten los modelos epidémicos fenomenológicos.

La Figura 6.7 muestra el mejor ajuste para cada una de las curvas del modelo SIR, en los 50 segundos iniciales de simulación del ataque, junto con los residuos obtenidos al aplicar el método de ajuste por mínimos cuadrados no lineal. Los resultados de la simulación corresponden nuevamente al primer caso de estudio del escenario 2 (*jamming* aleatorio a 50 paquetes/segundo contra el protocolo AODV cuando el nodo atacante está en el centro de la red de sensores inalámbricos).

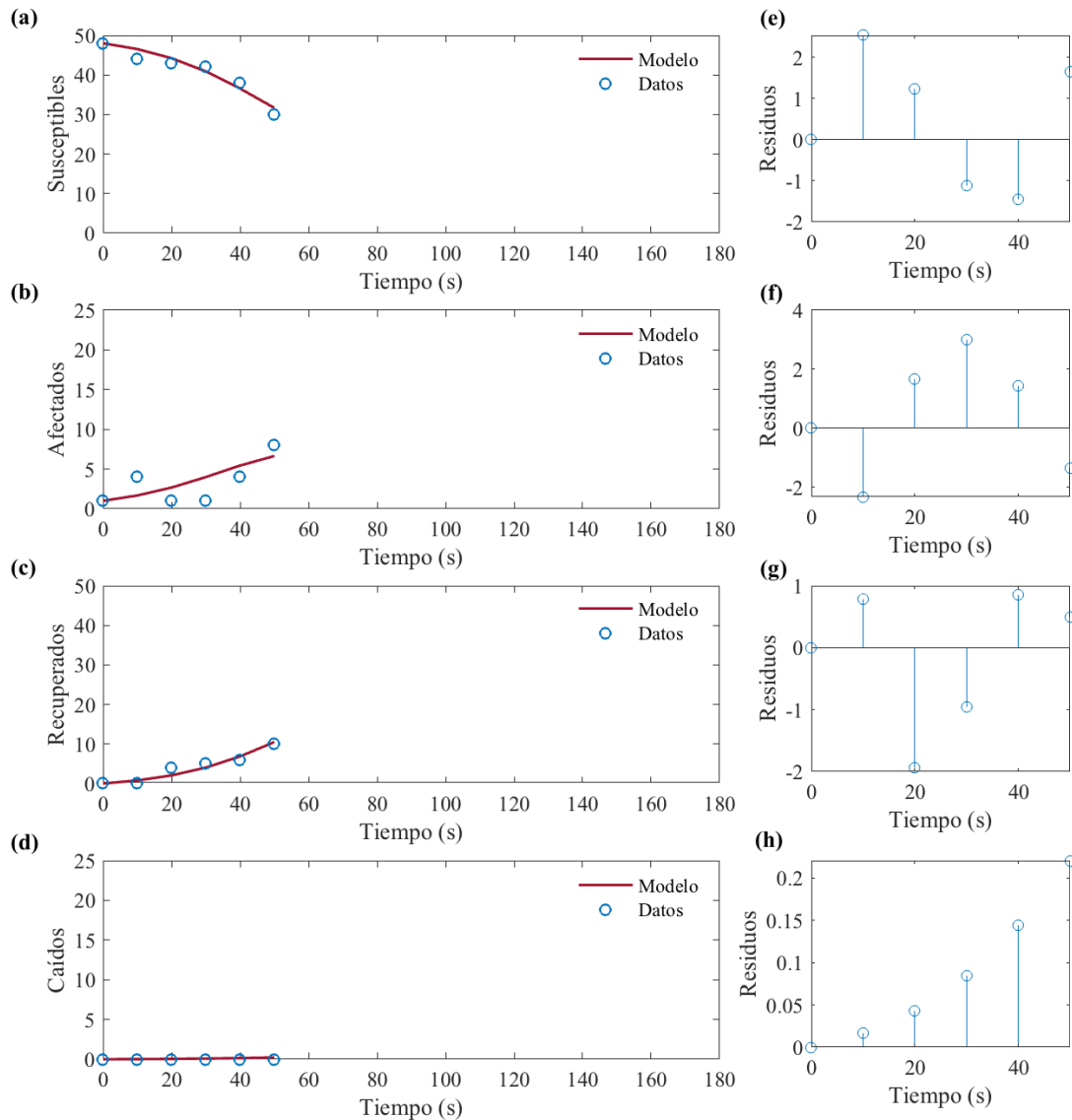


Figura 6.7. Ajuste del modelo en la etapa temprana del ataque *jamming* aleatorio a 50 paquetes/segundo contra el protocolo AODV cuando el nodo atacante está en el centro de la topología de la red.

En la Figura 6.7, las gráficas (a), (b), (c) y (d) muestran el mejor ajuste para la fase temprana del ataque de cada una de las curvas $dS(t)/dt$, $dI(t)/dt$, $dR(t)/dt$ del modelo SIR, junto con la curva de los nodos caídos $dD(t)/dt$. Los trazos en línea roja continua representan la fase temprana o periodo de calibración para cada una de las curvas característica del ataque, según el modelo propuesto para este experimento, mientras que los círculos azules representan los datos de referencia. En misma figura, las gráficas (e), (f), (g) y (h) muestra los residuos en función del tiempo. Según se observa, tanto el conjunto de curvas obtenidas en el experimento, como el patrón aleatorio de los residuos, sugiere, a priori, que el modelo ha proporcionado un ajuste razonablemente bueno para las distintas fases del ataque.

La Figura 6.8 muestra los histogramas (a), (b) y (c), con los valores correspondientes al 95% del intervalo de confianza obtenido para los parámetros β , γ , y ν , respectivamente. El histograma (d) representa el intervalo de confianza al 95%, del número reproductivo básico \mathcal{R}_0 , estimado con la Ecuación 5.6 descrita en el Capítulo 5. La obtención de los intervalos de confianza se realiza mediante la aplicación del método de *bootstrapping* ya descrito, y asumiendo una estructura de error basada en la distribución de *Poisson*. La cuantificación y obtención de estos intervalos de confianza, permite identificar la precisión con la que cada uno de los parámetros ha sido estimado en la fase inicial del ataque. En la figura se observa que, si al igual que con el experimento anterior, aquí también se obtiene un rango finito de valores alrededor de la media obtenida, en este caso los rangos del intervalo de confianza ligeramente más amplios. Esto es debido, fundamentalmente, a que para su obtención sólo se ha tenido en cuenta la fase inicial del ataque, por lo que la incertidumbre ha aumentado. En cualquier caso, el conjunto de parámetros ha sido estimado con una precisión aceptable.

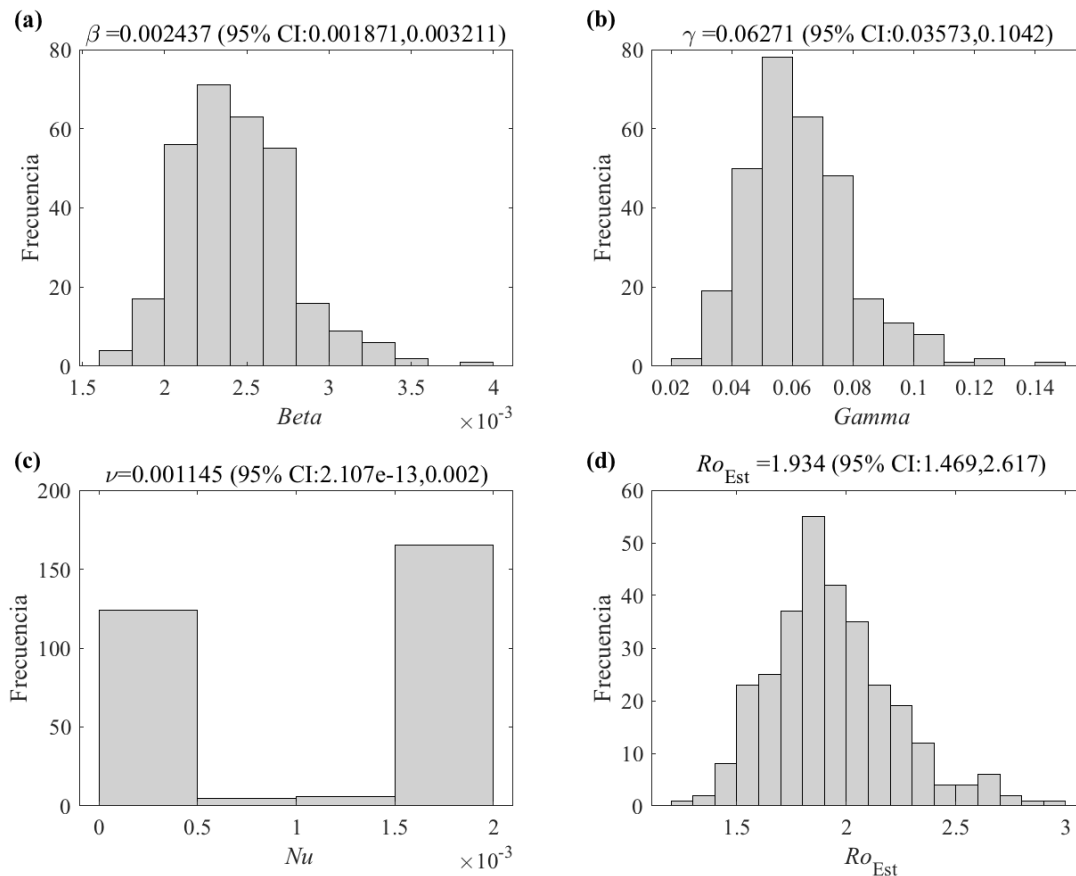


Figura 6.3. Histogramas de las distribuciones empíricas para las estimaciones del 95% de los intervalos de confianza de los parámetros β , γ , ν , y \mathcal{R}_0 .

Por otro lado, en la Figura 6.9 se han representado las curvas características del ataque pronosticadas por el modelo SIR tras el reajuste de los parámetros, junto con las curvas de la distribución de error generadas para la obtención del intervalo de confianza al 95% de dichos parámetros.

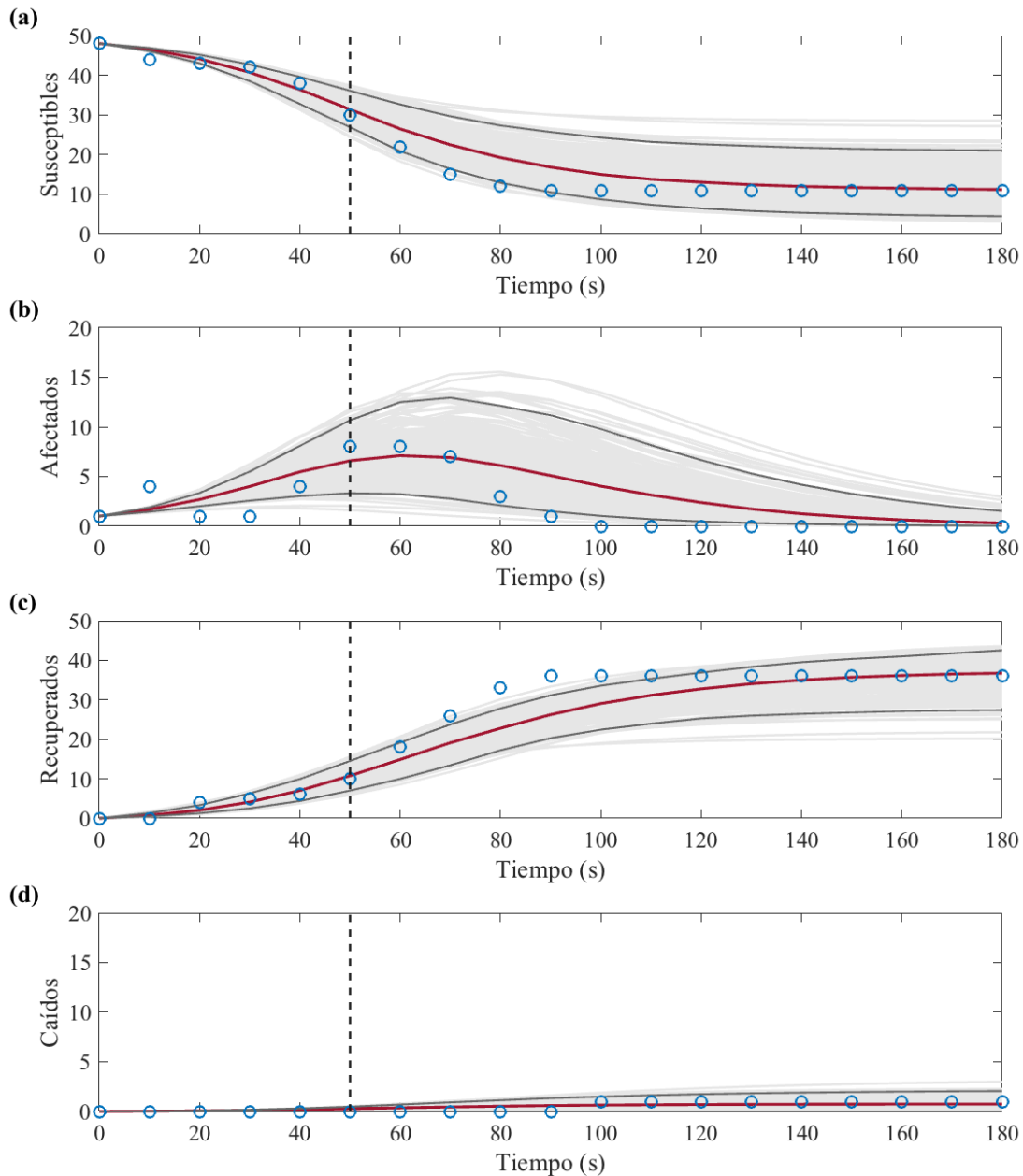


Figura 6.9. Pronóstico de la evolución del ataque dado por el modelo SIR, e intervalos de confianza obtenidos mediante *bootstrapping* para *jamming* aleatorio a 50 paquetes/segundo contra el protocolo AODV cuando el nodo atacante está en el centro de la topología de la red.

En la Figura 6.9, las gráficas (a), (b), (c) y (d) muestran el mejor ajuste para cada una de las curvas $dS(t)/dt$, $dI(t)/dt$, $dR(t)/dt$ del modelo SIR, junto con la curva de los

nodos caídos $dD(t)/dt$. La fase de calibración del modelo está separada de la fase de pronóstico con una línea vertical, por lo que todas las curvas a la derecha de esta línea corresponden a la evolución pronosticada del ataque. Los trazos en línea continua roja representan las curvas características del ataque para cada uno de los grupos de nodos, obtenidos experimentalmente según el modelo epidemiológico SIR utilizado, mientras que los círculos en azul representan los datos de referencia. Las líneas grises claro corresponden cada una de las 300 realizaciones o *bootstrapping* de las curvas de ataque pronosticadas, mientras que las dos líneas grises oscuro corresponden a los límites del 95% del intervalo confianza en torno al mejor ajuste de la curva pronosticada. Estas curvas permiten tanto la obtención del 95% del intervalo de confianza de los parámetros, como la identificación de la desviación potencial de éstos tras su reajuste.

Si bien en la Figura 6.9 se aprecia que los intervalos de confianza obtenidos son algo más amplios en comparación con los proporcionados por el modelo SIR retrospectivo, el conjunto de curvas características obtenidas experimentalmente indica que el modelo ha proporcionado una predicción de la evolución del ataque con una precisión razonablemente buena, tal y como se observa mediante la comparación del modelo con datos de referencia.

Como complemento a estos resultados, en la Figura 6.10 se presenta la curva de incidencia acumulada pronosticada $dD(t)/dt$ obtenida experimentalmente, junto con la incidencia acumulada obtenida de los datos de referencia. La fase de calibración del modelo está separada de la fase de pronóstico con una línea vertical, por lo que todas las curvas a la derecha de esta línea corresponden a la evolución pronosticada del ataque.

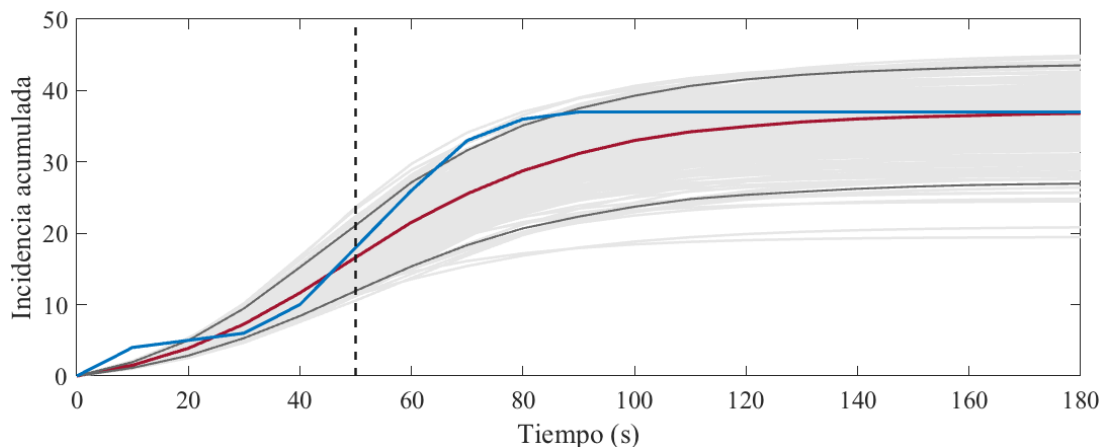


Figura 6.10. Curva pronosticada de la Incidencia acumulada y sus correspondientes intervalos de confianza obtenidos mediante *bootstrapping* para *jamming* aleatorio a 50 paquetes/segundo contra el protocolo AODV cuando el nodo atacante está en el centro de la topología de la red.

La línea continua roja representa la curva de incidencia acumulada pronosticada obtenida experimentalmente, mientras que línea continua azul representa la curva de incidencia acumulada obtenida según los datos de referencia. Las líneas grises claro corresponden cada una de las 300 realizaciones o *bootstrapping* de las curvas de ataque pronosticadas, mientras que las dos líneas grises oscuro corresponden a los límites del 95% del intervalo confianza en torno al mejor ajuste de la curva pronosticada. En este caso, también cabe destacar que el modelo ha proporcionado una predicción de la evolución del ataque con una precisión razonablemente buena.

Los resultados obtenidos experimentalmente para otros escenarios y tipos de ataque se han incluido en el Apéndice II y III.

6.2.3 Análisis de resultados de la simulación de ataques *jamming* mediante el modelo epidémico SIR determinista

Con objeto de dar una mayor solidez a la validación de la hipótesis planteada en esta investigación, y siguiendo la metodología descrita en el apartado anterior, se han desarrollado experimentos individuales para cada uno de los 27 ataques de referencia [22], obteniendo los parámetros que caracterizan a cada uno de ellos. Para cada escenario de ataque, se han simulado los 6 casos correspondientes a los ataques *jamming* aleatorio, y los 3 casos correspondientes a los ataques *jamming* reactivo. En base a estas simulaciones se ha realizado un análisis comparativo de los resultados del modelo SIR propuesto, con respecto a los datos de referencia.

En aras de no extender en exceso este Capítulo, en este apartado se presentan a modo de ejemplo los resultados de las 9 simulaciones correspondientes al escenario en el que el nodo atacante está en el centro de la topología de la red (escenario 2), para los ataques *jamming* aleatorio a 50 y 80 paquetes/segundo, y *jamming* reactivo. Estos resultados se han obtenido aplicando la metodología indicada en la sección 6.2.2. Los resultados experimentales obtenidos para el resto de escenarios y tipos de ataque se han incluido en los Apéndices II y III.

La Figura 6.11 presenta una comparativa en forma de histograma, de la evolución de los ataques. La Figura 6.11 (a) representa el número de nodos afectados o incidencia acumulada C_{∞} al final del ataque, considerando el intervalo de tiempo del experimento de 180 segundos. La incidencia acumulada permite analizar los efectos del

ataque sobre la población de nodos. Por otra parte, y para una mejor comprensión, en la Figura 6.11 (b) de esta misma figura se presentan los histogramas comparativos correspondientes al número de nodos susceptibles que han escapado del ataque S_∞ , igualmente tomados al final del tiempo del experimento. En la Figura 6.11 (a) las barras verticales de color gris representan la incidencia acumulada, y en la Figura 6.11 (b), representan a los nodos susceptibles al final del ataque obtenidos por el modelo SIR, mientras que las barras de color azul claro representan los datos de referencia. Para cada instante t , ha de verificarse que $S(t) + C(t) = N$, siendo $C(t) = \sum_{t=0}^{t=180} I(t)$.

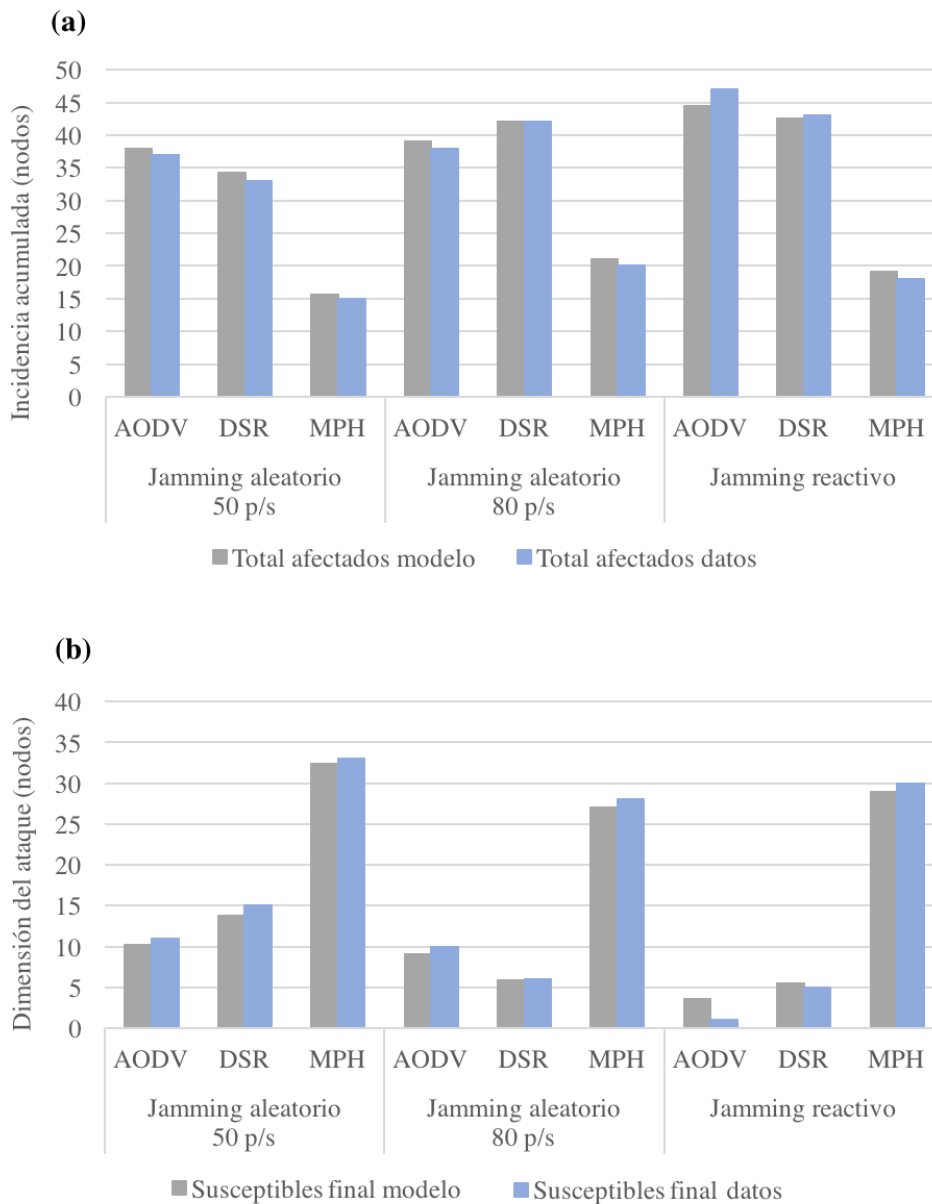


Figura 6.11. Histogramas comparativos de la incidencia acumulada (a) y número de nodos supervivientes o dimensión del ataque (b) para el segundo escenario de *jamming*.

En general, los resultados teóricos obtenidos por el modelo SIR se aproximan de manera precisa a los valores obtenidos de los datos de referencia. Por ejemplo, desde el punto de vista de la resiliencia de los protocolos estudiados, se observa que, para todos los tipos de ataques del escenario estudiado, el protocolo MPH parece mostrar una mejor resistencia frente al *jamming* que los protocolos AODV y DSR. Este hecho se aprecia en la incidencia acumulada C_∞ de la Figura 6.11 (a), donde, por ejemplo, para el *jamming* aleatorio a 50 paquetes/segundo contra AODV, se alcanzan valores de C_∞ que rondan los 38 nodos según el modelo, y para el mismo ataque contra DSR el valor de C_∞ es de unos 34 nodos. Por el contrario, este mismo ataque contra MPH arroja un valor de C_∞ de unos 15 nodos afectados, siendo inferior en algo más de un 50% a los valores obtenidos para los protocolos anteriores. En el caso del *jamming* aleatorio a 80 paquetes/segundo se observa un comportamiento análogo, pues para AODV y DSR se alcanzan valores de incidencia acumulada superiores a los 40 nodos afectados, mientras que MPH se mantiene entorno a los 20 nodos afectados. Por otra parte, en la Figura 6.11 (a), destaca especialmente la incidencia acumulada registrada por el ataque *jamming* reactivo para AODV y DSR con valores próximos a los 45 y 43 nodos acumulados respectivamente dados por el modelo (47 y 43 nodos respectivamente según los datos de referencia), mientras que el protocolo MPH se mantiene según el modelo entorno a los 19 nodos afectados (18 nodos según datos de referencia). Estos resultados confirman que, a priori, el protocolo MPH aporta una mayor resiliencia ante ataques que AODV y MPH. Para el resto de los casos y escenarios de ataque, se pueden realizar análisis similares.

Se pueden obtener conclusiones similares analizando los resultados experimentales obtenidos del número de nodos susceptibles S_∞ que escapan al ataque *jamming* para cada uno de los casos a estudio. Como se observa en la Figura 6.11 (b), para el segundo escenario, los ataques con un menor efecto negativo sobre la red inalámbrica se reflejan en un mayor número de nodos supervivientes al final de dichos ataques. Puede comprobarse la gran diferencia en el número de nodos que escapan al ataque en el caso de aquellos que incorporan el protocolo MPH, frente al número de los nodos que incorporan los protocolos AODV o MPH. Esto indica nuevamente, que la implementación del protocolo MPH, a priori, proporcionará a la red una mayor resiliencia frente a ataques *jamming* aleatorios y reactivos que el uso de protocolos como AODV o MPH.

Por otra parte, en la Figura 6.12 se ha presentado en forma de histograma, un análisis del impacto o severidad de los distintos tipos de ataque sobre la población de nodos, utilizando en este caso una comparativa del número reproductivo básico \mathcal{R}_0 como parámetro de estudio. El valor teórico dado por el modelo, se obtiene mediante la fórmula $\mathcal{R}_0 = \beta S_0 / (\gamma + \nu)$, y queda representado por las barras verticales gris claro. Para la obtención del \mathcal{R}_0 estimado tanto del modelo SIR, como por los datos de referencia, se ha utilizado la Ecuación 5.6, descrita en el Capítulo 5, donde intervienen los valores de S_0 y S_∞ . Estos valores se representan por barras verticales de color azul claro y naranja, respectivamente.

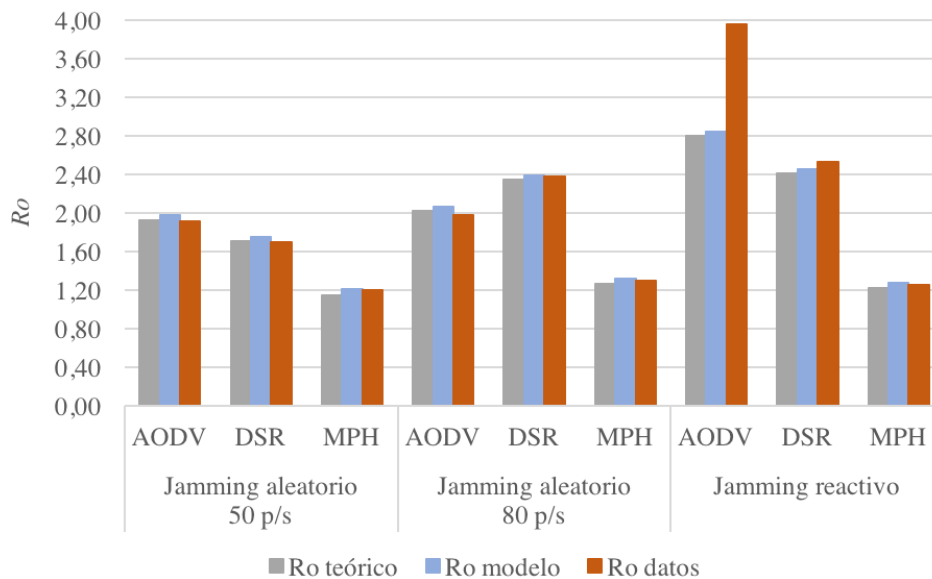


Figura 6.12. Histogramas comparativos de la severidad del ataque \mathcal{R}_0 , para *jamming* aleatorio y reactivo, para el segundo escenario, cuando el atacante está en el centro de la topología de la red.

En la Figura 6.12 se observa, en primer lugar, que los resultados experimentales obtenidos por el modelo SIR para \mathcal{R}_0 se ajustan con bastante exactitud a los resultados obtenidos de los datos de referencia, salvo para el caso del ataque de *jamming* reactivo contra el protocolo AODV. Esta discrepancia se debe a una subestimación puntual de los parámetros por parte del modelo SIR. En cualquier caso, la comparativa muestra claramente que, al igual que en epidemiología, cuanto mayor sea el número reproductivo básico asociado al ataque, mayor será la propagación de dicho ataque a través de la red. Esta propagación se reflejará en una mayor incidencia acumulada C_∞ , o bien en un menor número de nodos susceptibles S_∞ que escapan al ataque.

Por otra parte, se puede realizar un estudio más detallado del número reproductivo básico en base a los parámetros que lo componen. Además del número inicial de individuos susceptibles S_0 que componen la población a estudio, \mathcal{R}_0 depende de la tasa de contagio β , de la tasa de nodos caídos ν , y del tiempo de recuperación o persistencia del ataque de $1/\gamma$. Según los valores obtenidos experimentalmente para los parámetros β y ν , el orden de magnitud de éstos no permite un análisis comparativo claro para el estudio del número reproductivo básico asociado al ataque. Por ejemplo, para el escenario actual, los valores de β oscilan entre 0.00259 (*jamming* reactivo contra el protocolo DSR), y 0.00346 (*jamming* aleatorio a 50 paquetes/segundo contra el protocolo MPH), siendo estos valores mucho menores para el parámetro ν . Además, tal y como se describió en el Capítulo 5 (apartado 5.4) la tasa de contagio β puede descomponerse en dos parámetros, donde k es el número promedio de conexiones entre nodos y representa, la probabilidad de que el ataque afecte al menos a un nodo de la red. Y, por otra parte, la transmisibilidad λ que representa la probabilidad de que el ataque *jamming* sea efectivo dado el contacto entre un nodo susceptible y un infectado, siendo la tasa de contagio para este modelo $\beta = \lambda \cdot k$. El factor k queda definido por la topología de la red y el número de nodos N , siendo $k = 1 - e^{-Np}$, con $p = \pi r_0^2 / A$, donde r_0 es el rango de transmisión para cada nodo y A es el área total de la red. Fijados estos parámetros para la red a estudio, se obtiene que $k \approx 0.9848$, por lo que el estudio del parámetro λ , también resultaría poco clarificador. Sin embargo, los resultados experimentales obtenidos para el parámetro γ , si proporcionan un medio para realizar un análisis comparativo del número reproductivo básico asociado al ataque. En concreto, el siguiente análisis se centra en el estudio del parámetro $1/\gamma$.

Como se indicó anteriormente, cuanto mayor sea el número reproductivo básico asociado al ataque, mayor será la propagación de dicho ataque a través de la red. Esta mayor propagación se reflejará, tanto en un mayor número de nodos afectados o incidencia acumulada, como en una mayor duración o persistencia del ataque, definida por el parámetro $1/\gamma$, el cual representa el tiempo de recuperación de los nodos. En la Figura 6.13 se ha representado una comparativa del parámetro $1/\gamma$ para los diferentes casos del segundo escenario de ataques *jamming*, donde el cuadrado rojo representa el valor medio de dicho parámetro, mientras que la línea vertical negra y sus círculos asociados, representan el valor máximo y mínimo del 95% de intervalo de confianza.

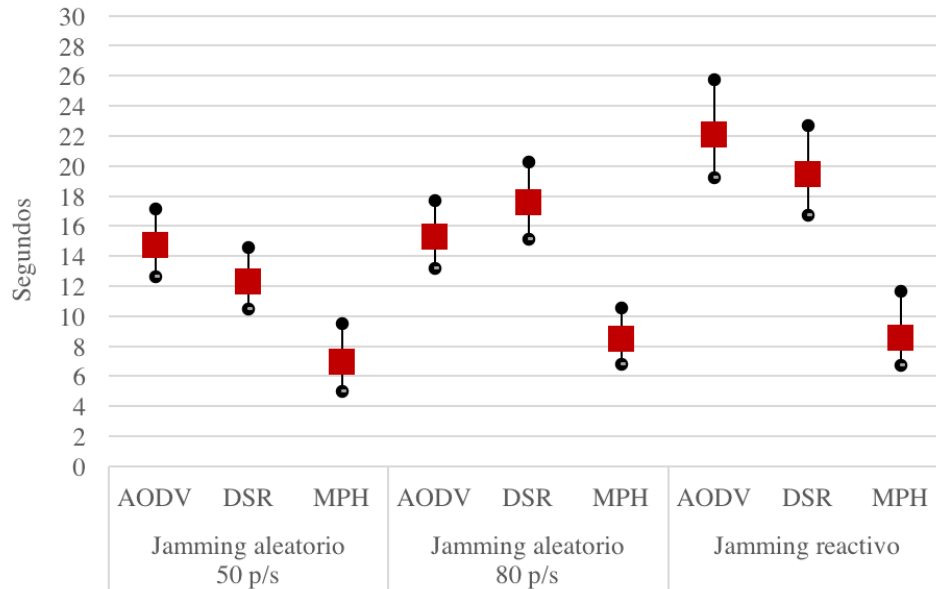


Figura 6.13. Comparativa de la persistencia del ataque, factor $1/\gamma$, para los diferentes casos del segundo escenario.

Los resultados experimentales obtenidos confirman que cuanto mayor es el tiempo de recuperación del ataque (menores valores de γ), mayor es el número reproductivo básico y, por tanto, mayor será la propagación y la incidencia de dicho ataque a través de la red. En efecto, desde el punto de vista de la resiliencia se observa nuevamente que, para todos los tipos de ataques del escenario estudiado, el protocolo MPH muestra una mejor resistencia frente a los diferentes tipos de *jamming* que, AODV y DSR. Este hecho se aprecia en que los nodos equipados con estos últimos protocolos tienen mayores tiempos de recuperación, en comparación con los tiempos de recuperación de los nodos equipados con MPH. Por ejemplo, en el caso del *jamming* reactivo, el valor del parámetro $1/\gamma$ es superior a 20 segundos para los nodos equipados con AODV y DSR, mientras que apenas llega a los 10 segundos para MPH. En concreto, el ataque de *jamming* reactivo contra los nodos equipados con el protocolo AODV aparece nuevamente como el más dañino, con un tiempo de recuperación medio de los nodos $1/\gamma = 22.08$ segundos.

Con esta última comparativa, se concluye, por lo tanto, que los resultados experimentales obtenidos en aplicación del modelo SIR están, en total consonancia los datos de referencia. Además, cabe resaltar, que los valores de $\mathcal{R}_0 > 1$ dados por los modelos propuestos, confirman que al igual que en epidemiología, el ataque *jamming* se comporta como un brote epidémico, entre la población de nodos de la red inalámbrica.

6.3 Aplicación del Modelo de Crecimiento Generalizado y del Modelo de Crecimiento Logístico Generalizado para la predicción de la propagación de ataques *jamming*

En este apartado del experimento, se han utilizado los modelos de Crecimiento Generalizado (*Generalized Growth Model*, GGM) y de Crecimiento Logístico Generalizado (*Generalized Logistic Growth Model*, GLGM) para la estimación de los parámetros principales que caracterizan la propagación de los ataques *jamming* contra la red inalámbrica a estudio. En el primer modelo, se han determinado r y p como parámetros que denotan la tasa de crecimiento intrínseca y el factor de desaceleración del crecimiento. El segundo de los modelos, además de los parámetros r y p , aporta un nivel de saturación que representa un límite superior para el crecimiento del ataque. Este límite o capacidad de carga K , representa en este modelo el tamaño final del ataque, esto es, el número total de nodos afectados tras el ataque *jamming*.

En ambos modelos se requiere una calibración inicial, por lo que se ha definido una fase temprana del ataque con el fin de poder realizar un ajuste inicial de los parámetros. De forma general, la calibración previa del modelo GGM con respecto a los datos de referencia, proporciona un ajuste adecuado para las fases tempranas del ataque. Sin embargo, GGM solo considera el crecimiento ilimitado de los nodos afectados, por lo que no es adecuado modelar un ataque que ha entrado o superado su pico de incidencia. Por otra parte, el modelo de crecimiento GLGM proporciona un ajuste poco preciso en las etapas iniciales del ataque, sin embargo, aporta el límite superior K , estimando el número máximo de nodos afectados, y proporcionando una mejor caracterización de la dinámica del ataque una vez superado al pico de éste. Por lo tanto, ambos modelos son complementarios, de modo que, para la fase temprana del ataque, se emplea GGM obteniendo los parámetros r y p . Luego estos parámetros se pasan como valores de referencia para resolver el modelo GLGM y obtener el mejor ajuste del ataque. Este concepto de ensamblaje de diferentes modelos de crecimiento se ha empleado originalmente para el estudio de la dinámica de epidemias, tal y como queda reflejado en trabajos como [24], [118], [119], [131].

Para llevar a cabo este experimento se han resuelto las ecuaciones diferenciales 5.18 y 5.20, de cada uno de los modelos, ya descritos en el Capítulo 5. De su resolución se obtienen la curva $C'(t)$ que representa la incidencia o número de nodos inalcanzables

o afectados para cada instante t , y la curva $C(t)$, que representa el número acumulado de nodos inalcanzables en el tiempo t . Al igual que en la sección anterior, para la obtención de los parámetros caracterizadores de los diferentes casos de ataques, se aplica el método ajuste de mínimos cuadrados no lineal. Cabe señalar que el modelo GLGM es bastante sensible a la definición inicial del intervalo de tiempo elegido para la fase temprana del ataque, por lo que, se realizaron simulaciones previas con el fin de comprender mejor la dinámica de este ciberataque.

Posteriormente, se cuantifica el intervalo de confianza del 95% del de los parámetros estimados, para identificar la desviación potencial o incertidumbre de éstos, utilizando el método de *bootstrapping* paramétrico ya descrito en el Capítulo 5. Básicamente, en esta fase se vuelven a estimar los parámetros del modelo utilizando nuevamente el método de mínimos cuadrados, y asumiendo que la serie temporal de datos sigue una estructura de error de distribución de *Poisson*, centrada en la media de los puntos temporales de cada observación. Para ello, se muestrean repetidamente los puntos de la curva obtenida en la fase anterior (se realizan 300 muestreos), obteniendo múltiples observaciones y generando conjuntos de datos sintéticos. Posteriormente, se aplica el método de mínimos cuadrados sobre cada una de estas 300 realizaciones, obteniendo una nueva estimación de los parámetros que minimizan la suma de los cuadrados de las diferencias entre el modelo deseado y los datos obtenidos de las 300 curvas generadas.

El intervalo de confianza del 95% para el conjunto de parámetros se obtiene, tal y como se indicó en el Capítulo 5, aplicando la función de cálculo de *cuantiles*, corresponde al paquete MCMCSTAT que contiene un conjunto de funciones de MATLAB para análisis estadísticos de modelos matemáticos [152].

De los diferentes análisis y datos obtenidos tras este experimento, se dispone de un conjunto de resultados significativos que caracterizan cada uno de los casos de ataque, tales como los parámetros estimados r , p y K , el número máximo de nodos afectados, y una estimación del número reproductivo básico \mathcal{R}_0 , en el caso de GLGM.

6.3.1 Estudio predictivo de la propagación de ataques *jamming* mediante el Modelo de Crecimiento Generalizado (GGM)

Con el fin de no extender este Capítulo, se expone en este apartado los resultados obtenidos del experimento relativo al caso de estudio 10, correspondiente al segundo escenario de ataque donde se ejecuta un *jamming* aleatorio a 50 paquetes/segundo contra el protocolo AODV cuando el nodo atacante está en el centro de la red de sensores inalámbricos. En este experimento, el ataque se ha simulado y analizado sobre un periodo de tiempo de 150 segundos, estableciendo la fase inicial del ataque para la calibración del modelo en 50 segundos, con un número inicial de casos reportados $C_0 = 1$. Los resultados experimentales obtenidos para otros tipos de ataque y escenarios se han incluido en el Apéndice II y III.

En primer lugar, se han establecido unos valores estimativos para r y p , para la calibración la fase inicial del ataque, presentados en la Tabla 6.6. Posteriormente, se aplica el método ajuste de mínimos cuadrados no lineal, obteniendo una estimación de los parámetros característicos minimizando la suma del cuadrado de las diferencias entre el modelo propuesto y el conjunto de datos de ataques *jamming* de referencia.

Parámetro	Valor esperado	Límite inferior	Límite superior
Tasa de crecimiento intrínseca r	0.1	0.01	1.0
Factor de desaceleración del crecimiento p	0.6	0.01	1.2

Tabla 6.6. Límites y valores esperados inicial para los parámetros r y p .

La Figura 6.14 (a) muestra el mejor ajuste del modelo GGM para la fase inicial del ataque, obtenida en base a una primera estimación de los parámetros r y p , al aplicar el método de ajuste por mínimos cuadrados no lineal. Asimismo, los residuos obtenidos se presentan en la Figura 6.14 (b). El trazo de línea continua roja de la Figura 6.14 (a) representa la curva característica de crecimiento de nodos afectados obtenida por el experimento para la fase temprana del ataque, y los círculos azules representan los datos de referencia. En la Figura 6.14 (b), el patrón aleatorio en función del tiempo de los residuos sugiere que el modelo GGM ha proporcionado un ajuste razonablemente bueno en la fase de crecimiento inicial del ataque.

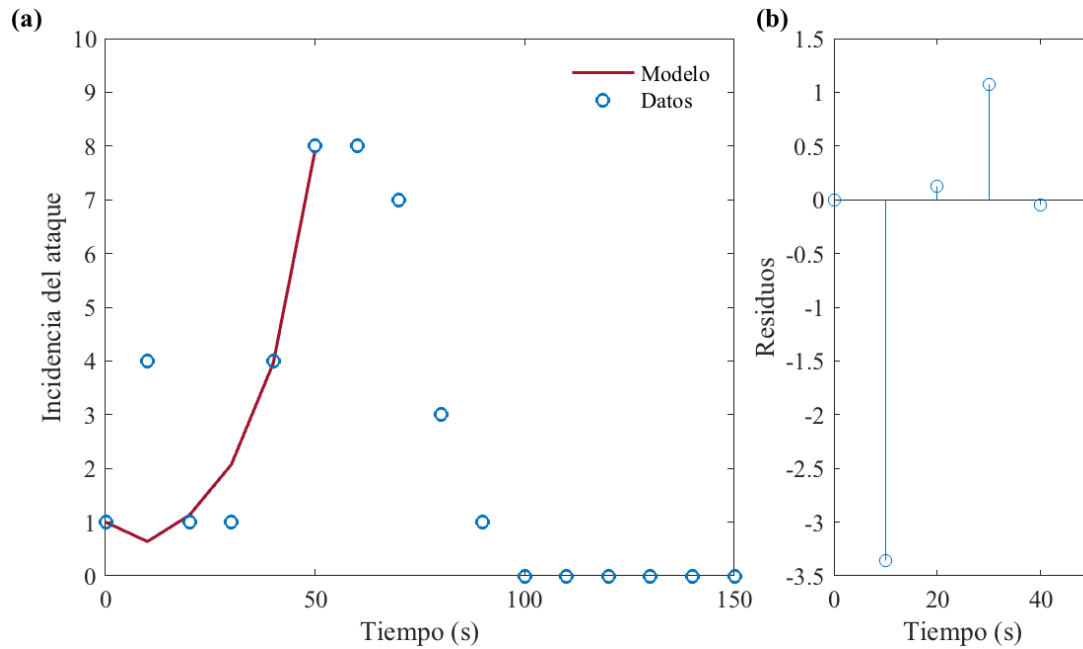


Figura 6.14. Mejor ajuste del modelo GGM para la fase inicial del ataque (a), junto con los residuos obtenidos (b), al aplicar el método de ajuste por mínimos cuadrados no lineal.

Una vez obtenida la estimación de los parámetros en la fase inicial del ataque, se construye un pronóstico a corto plazo mediante la extensión de la incertidumbre del sistema. Para ello, se utiliza la incertidumbre asociada a las estimaciones de parámetros calculadas previamente. De esta forma, el estado del sistema obtenido en la fase inicial del ataque, se propaga a un horizonte de T unidades de tiempo hacia adelante.

En la Figura 6.15 (a) y (b) se muestran los histogramas de las distribuciones empíricas para las estimaciones de parámetros y los valores correspondientes al intervalo de confianza del 95% de los parámetros r y p respectivamente, después del reajuste de los parámetros obtenidos en la fase temprana del ataque. Para el reajuste de los parámetros también se ha empleado la técnica de *bootstrapping*, asumiendo una distribución de error de *Poisson* con $m = 300$ realizaciones. En los histogramas se puede observar un rango finito de valores alrededor de la media obtenida, lo que indica que el conjunto de parámetros ha sido estimado con una precisión aceptable.

En la Figura 6.15 (c), se presenta el pronóstico a corto plazo de la evolución del ataque. La línea roja corresponde al mejor ajuste de la curva de ataque pronosticada por el experimento para el modelo GGM, mientras que los círculos azules representan los datos de referencia. Las líneas negras corresponden a los límites de confianza del 95% en torno al mejor ajuste de la curva pronosticada, y las líneas grises corresponden a las m realizaciones de *bootstrapping* de las curvas de ataque pronosticadas. El período de

calibración se ha separado del período de pronóstico con una línea negra punteada vertical, por lo que todas las curvas a la derecha de esta línea corresponden a la evolución pronosticada del ataque. El valor obtenido de $p = 1$, indica que este caso se caracteriza por dinámica de crecimiento exponencial, con $C(t) = C_0 e^{rt}$, siendo C_0 el número inicial de nodos afectados.

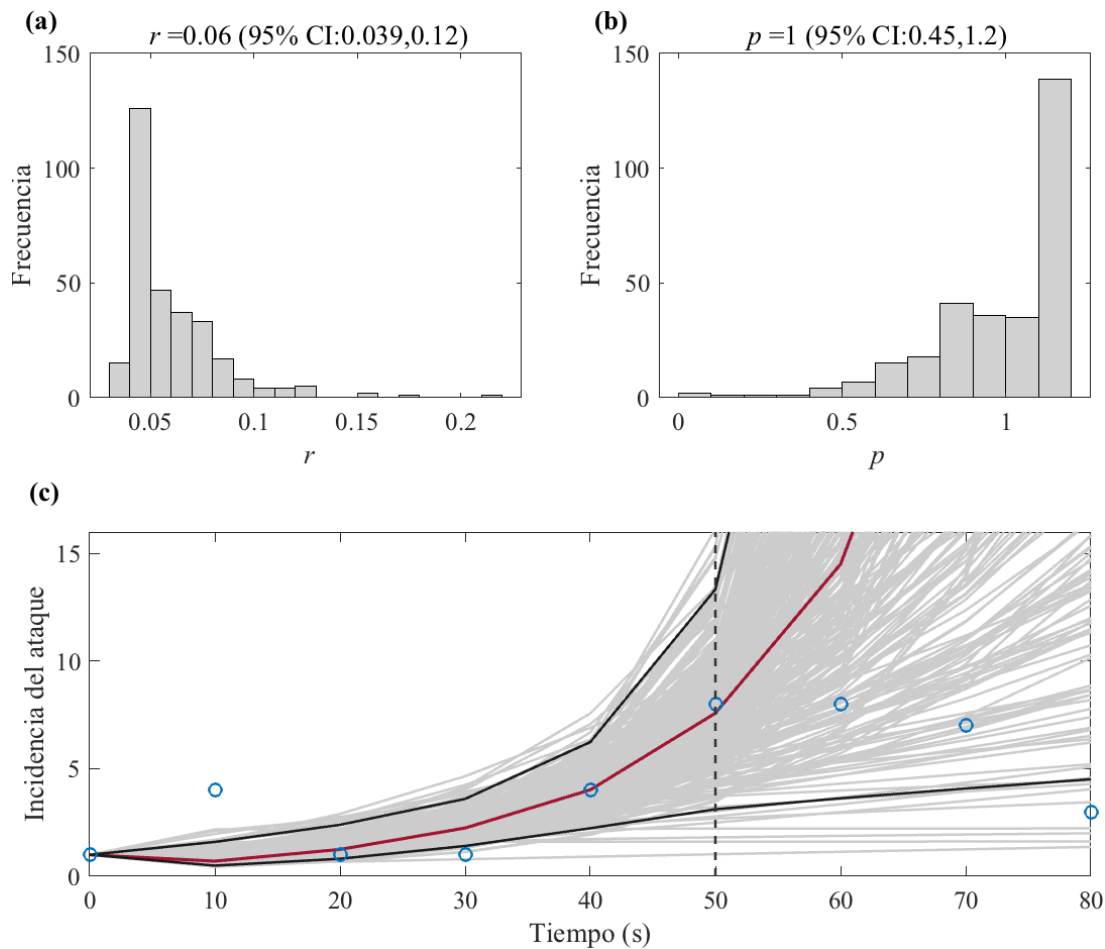


Figura 6.15. Histogramas de distribuciones empíricas para las estimaciones de parámetros r (a), y p (b) correspondientes al intervalo de confianza del 95%, y mejor ajuste de la curva de ataque (c), pronosticada en el experimento para el modelo GGM.

Tal y como ya se adelantó, el modelo GGM proporciona un buen ajuste en etapas tempranas del ataque, sin embargo, el modelo estima un crecimiento exponencial ilimitado de los nodos afectados. Este crecimiento exponencial queda reflejado en la Figura 6.16, donde se ha representado la curva $C(t)$ característica del ataque correspondiente al número acumulado de nodos inalcanzables en el tiempo. Dado el crecimiento exponencial de la curva, el tiempo de la representación se ha limitado a 80 segundos.

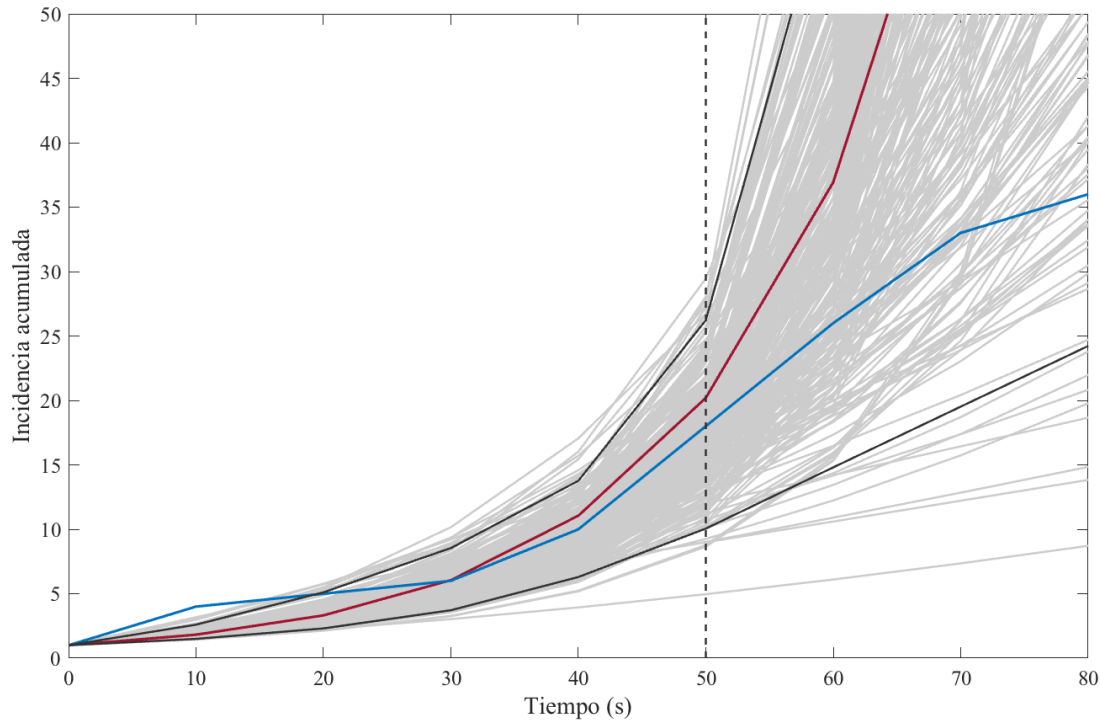


Figura 6.16. Mejor ajuste de la curva $C(t)$ pronosticada por el modelo GGM.

La línea continua roja corresponde al mejor ajuste de la curva de ataque pronosticada por el experimento para el modelo GGM, mientras que la línea continua azul representan los datos de nodos afectados acumulados proporcionados por los datos de referencia. Las líneas negras corresponden a los límites de confianza del 95% en torno al mejor ajuste de la curva pronosticada, y las líneas grises corresponden a las m realizaciones de *bootstrapping* de las curvas de ataque pronosticadas. El período de calibración está separado del período de pronóstico con una línea negra vertical, por lo que todas las curvas a la derecha de esta línea corresponden a la evolución pronosticada del ataque. Las figuras 6.15 (c) y 6.16, muestran la principal limitación del modelo GGM, pues éste considera un crecimiento ilimitado de nodos afectados. Este supuesto poco realista, puede llevar a una extrapolación errónea en los resultados pronosticados. Incluso durante el experimento, se pudo comprobar que, al aumentar el tiempo de simulación por encima de los 100 segundos, el número de nodos afectados acumulados que se obtiene, es mayor que la propia población inicial de nodos que componen la red inalámbrica, esto es, $C_\infty \gg S_0$, lo que proporciona un escenario poco realista.

6.3.2 Estudio predictivo de la propagación de ataques *jamming* mediante el Modelo de Crecimiento Logístico Generalizado (GLGM)

Para sacar partido al ajuste proporcionado por GGM en las fases tempranas del ataque, se han utilizado los parámetros obtenidos con dicho modelo pasándolos como valores de referencia para resolver el modelo GLGM y obtener un mejor pronóstico de la evolución del ataque en todas sus etapas. Como ejemplo, se ha tomado nuevamente el caso de estudio 10, correspondiente al segundo escenario de ataque donde se lanza un *jamming* aleatorio a 50 paquetes/segundo contra el protocolo AODV cuando el nodo atacante está en el centro de la red de sensores inalámbricos. Este ataque se ha simulado y analizado sobre un periodo de tiempo de 150 segundos, estableciendo en 50 segundos la fase inicial del ataque para la calibración del modelo, con un número inicial de casos reportados $C_0 = 1$. Los resultados experimentales obtenidos para otros escenarios y tipos de ataque aleatorio se han incluido en los Apéndices II y III.

En primer lugar, se han establecido los valores estimativos para r , p y K , para la calibración de la fase inicial del ataque, teniendo en cuenta que los valores esperados para r y p , son los obtenidos en el apartado anterior. El parámetro K se ha estimado en un 90% el número máximo de nodos afectados de la red (43), un mínimo de un nodo afectado, y un valor esperado del 50% de nodos de la red afectados (24). Estos valores se presentan en la Tabla 6.7. Posteriormente, aplicando el método ajuste de mínimos cuadrados no lineal, se obtiene una estimación de los parámetros característicos minimizando la suma del cuadrado de las diferencias entre el modelo propuesto y el conjunto de datos del ataque de referencia.

Parámetro	Valor esperado	Límite inferior	Límite superior
Tasa de crecimiento intrínseca r	0.06	0.039	0.13
Factor de desaceleración del crecimiento p	1.0	0.42	1.2
Capacidad de carga K (nº de nodos)	24	1	43

Tabla 6.7. Límites y valores esperados inicial para los parámetros r , p (tomados del modelo GGM), y K .

La Figura 6.17 (a) muestra el mejor ajuste del modelo GLGM para la fase inicial del ataque, obtenida en base a una primera estimación de los parámetros r , p y K , al

aplicar el método de ajuste por mínimos cuadrados no lineal. Asimismo, los residuos obtenidos se presentan en la Figura 6.17 (b).

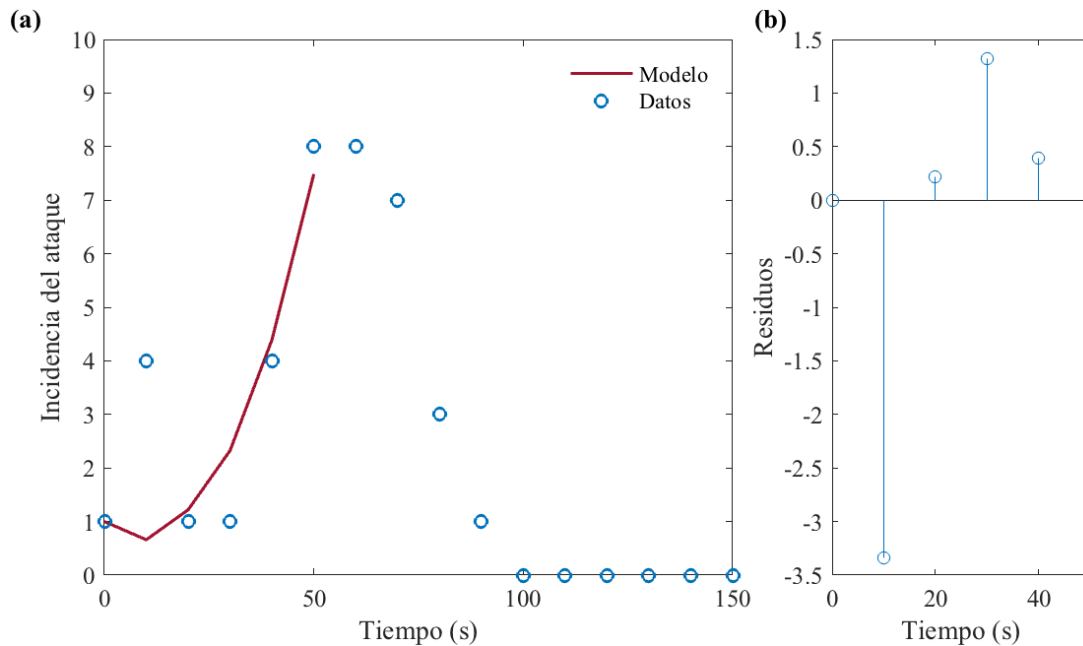


Figura 6.17. Mejor ajuste del modelo GLGM para la fase inicial del ataque (a), junto con los residuos obtenidos (b), al aplicar el método de ajuste por mínimos cuadrados no lineal.

El trazo de línea continua roja de la Figura 6.17 (a) representa la curva característica de crecimiento de nodos afectados, estimada experimentalmente para la fase temprana del ataque, mientras que los círculos azules representan los datos de referencia. El patrón aleatorio en función del tiempo de los residuos presentados en la Figura 6.17 (b), sugiere que el modelo GLGM ha proporcionado un ajuste razonablemente bueno en la fase de crecimiento inicial del ataque.

Una vez obtenida la estimación de los parámetros en la fase inicial del ataque, se construye un pronóstico a corto plazo mediante la extensión de la incertidumbre del sistema. Para ello, se utiliza la incertidumbre asociada a las estimaciones de parámetros calculadas previamente. De esta forma, el estado del sistema obtenido en la fase inicial del ataque, se propaga a un horizonte de T unidades de tiempo hacia adelante.

En la Figura 6.18 (a), (b) y (c) se muestran los histogramas de las distribuciones empíricas para las estimaciones de parámetros y los valores correspondientes al intervalo de confianza del 95% correspondientes para r , p y K , respectivamente, después del reajuste de los parámetros obtenidos en la fase temprana del ataque. Para el reajuste de los parámetros también se ha empleado la técnica de *bootstrapping*, asumiendo una distribución de error de *Poisson* con $m = 300$ realizaciones. En los histogramas se puede

observar un rango finito de valores alrededor de la media obtenida, lo que indica que el conjunto de parámetros ha sido estimado con una precisión aceptable. El valor de p ligeramente superior a 1 dado por el ajuste del modelo GLGM, indica que caso de ataque *jamming* estudiado se caracteriza en su fase inicial por una dinámica de crecimiento súper-exponencial [128].

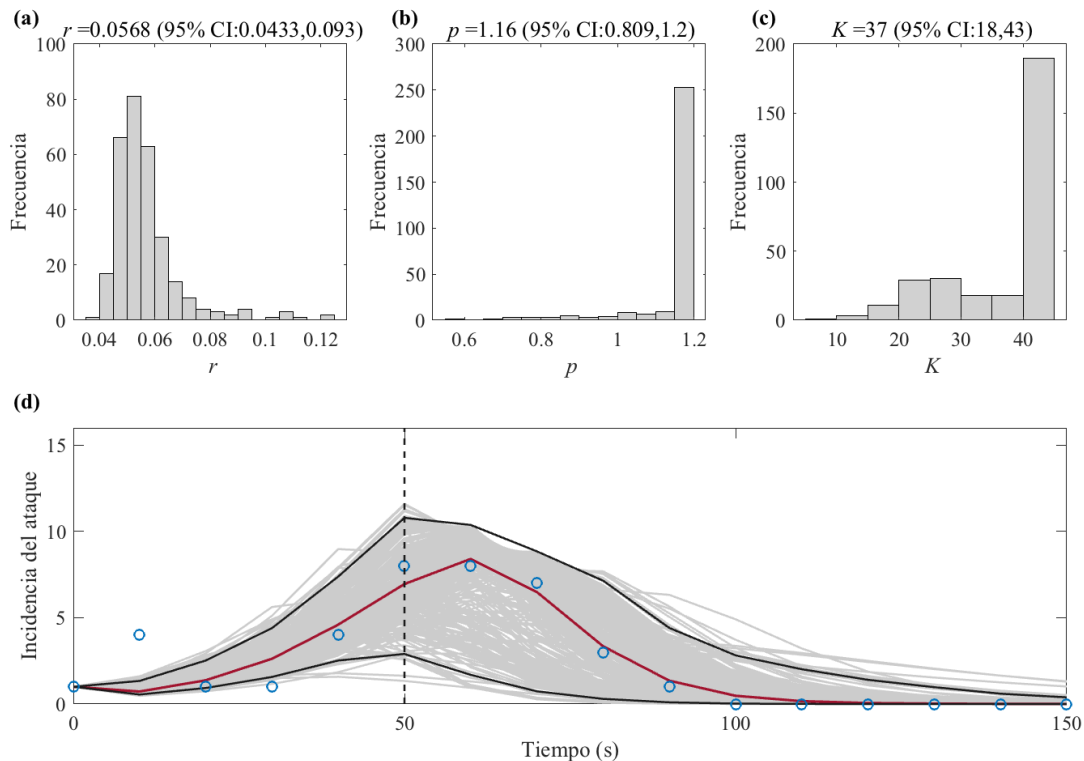


Figura 6.18. Histogramas de las distribuciones empíricas para las estimaciones de parámetros al 95%, y mejor ajuste de la curva de ataque pronosticada por el modelo GLGM.

En la Figura 6.18 (d), se presenta el pronóstico a corto plazo de la evolución del ataque. La línea roja corresponde al mejor ajuste de la curva de ataque pronosticada por el experimento para el modelo GLGM, mientras que los círculos azules representan los datos de referencia. Las líneas negras corresponden a los límites de confianza del 95% en torno al mejor ajuste de la curva pronosticada, y las líneas grises corresponden a las m realizaciones de *bootstrapping* de las curvas de ataque pronosticadas. El período de calibración se ha separado del período de pronóstico con una línea negra punteada vertical, por lo que todas las curvas a la derecha de esta línea corresponden a la evolución pronosticada del ataque.

Tal y como se esperaba, el modelo GLGM ha proporcionado un buen ajuste en las etapas posteriores al pico del ataque, ya que la incorporación del parámetro K evita un crecimiento exponencial ilimitado de los nodos afectados. Esta capacidad de carga

máxima del sistema queda reflejada en la Figura 6.19, donde se ha representado la curva $C(t)$ característica del ataque correspondiente al número acumulado de nodos afectados o inalcanzables, para un periodo de tiempo del ataque de 120 segundos.

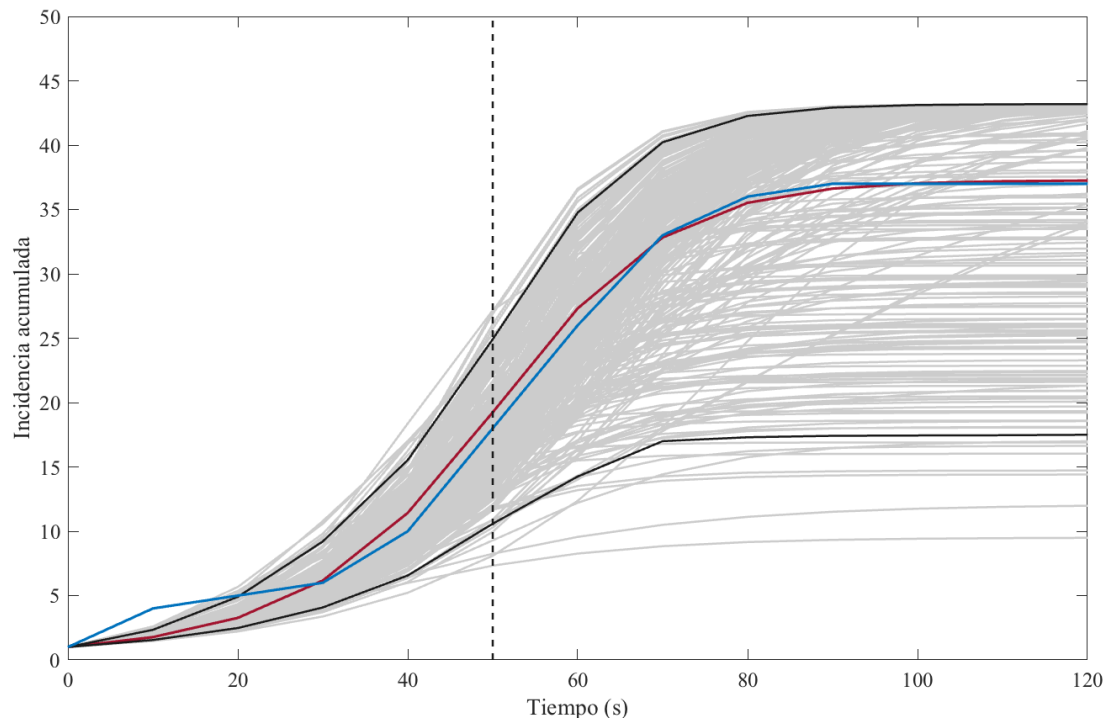


Figura 6.19. Mejor ajuste de la curva $C(t)$ pronosticada por el modelo GLGM.

La línea continua roja corresponde al mejor ajuste de la curva de ataque pronosticada experimentalmente por del modelo GLGM, mientras que la línea continua azul representan los nodos afectados acumulados proporcionados por los datos de referencia. Las líneas negras corresponden a los límites de confianza del 95% en torno al mejor ajuste de la curva pronosticada, y las líneas grises corresponden a las m realizaciones de *bootstrapping* de las curvas de ataque pronosticadas. El período de calibración está separado del período de pronóstico con una línea negra vertical, por lo que todas las curvas a la derecha de esta línea corresponden a la evolución pronosticada del ataque. En este caso se comprueba que con la utilización combinada de los modelos GGM y GLGM los resultados pronosticados de la evolución del ataque se ajustan al número de nodos afectados acumulados proporcionados por datos de referencia.

Por último, como ya se indicó anteriormente, el parámetro K proporciona el tamaño final del ataque, dado como el número total de nodos afectados siendo crucial para generar pronósticos tras el pico del ataque. Tal y como se describe en el Capítulo 5, para $K > 0$, este parámetro, puede vincularse al número reproductivo básico \mathcal{R}_0 obtenido

con el modelo SIR. En efecto, la Ecuación 5.21 permite obtener una relación entre el número reproductivo básico y el tamaño final del ataque, en función de la población inicial de nodos N , del número inicial de nodos susceptibles S_0 , y del número final de nodos que escaparon del ataque S_∞ . Asumiendo que al inicio del ataque se tiene $N \approx S_0$ nodos, y que $K = S_0 - S_\infty$. En la Tabla 6.8 se presenta una comparativa de los valores de \mathcal{R}_0 obtenidos con cada uno de los modelos descritos hasta ahora. Entre paréntesis se indica el apartado de este Capítulo del que se extrae el resultado.

Parámetro	Valor
\mathcal{R}_0 teórico SIR ^(6.2.2)	1.92661 (95% CI: 1.804902, 2.068928)
\mathcal{R}_0 estimado modelo SIR ^(6.2.2)	1.97114 (95% CI: 1.85002, 2.109139)
\mathcal{R}_0 teórico SIR ^(6.2.3)	1.90493 (95% CI: 1.42232, 2.641423)
\mathcal{R}_0 estimado modelo SIR ^(6.2.3)	1.93365 (95% CI: 1.46871, 2.61744)
\mathcal{R}_0 estimado modelo GLGM	1.93030 (95% CI: 1.24431, 2.558427)
\mathcal{R}_0 estimado datos referencia	1.91131

Tabla 6.8. Estimación por diferentes modelos epidémicos del número reproductivo básico \mathcal{R}_0 para el ataque *jamming* aleatorio a 50 paquetes/segundo contra el protocolo AODV para el segundo escenario de ataque.

El valor estimado por el modelo GLGM, tomando el valor de K resultante del pronóstico de la evolución del ataque, es de $\mathcal{R}_0 = 1.9303$ (95% CI: 1.2443, 2.5584), siendo el obtenido según los datos de referencia $\mathcal{R}_0 = 1.9113$.

En conjunto, todos los modelos propuestos en el experimento han realizado una caracterización del ataque satisfactoria proporcionando valores de \mathcal{R}_0 en línea con el obtenido de los datos de referencia. Además, cabe resaltar, que los valores de $\mathcal{R}_0 > 1$ dados por los modelos propuestos, confirman que al igual que en epidemiología, el ataque *jamming* se propagará en forma de brote epidémico dentro de la red inalámbrica, tal y como se ha demostrado mediante los experimentos anteriores.

6.3.3 Análisis de resultados de los experimentos de ataques *jamming* mediante Modelos de Crecimiento Generalizado

Al igual que se realizó en la sección anterior, con objeto de dar una mayor solidez a la validación del modelo propuesto, se han realizado un total de 27 experimentos para simular de forma individual cada uno de los 27 ataques indicados en [22]. De este modo se han obtenido los parámetros que caracterizan a cada uno de estos ataques. Para cada uno de los escenarios, se han simulado los 6 casos correspondientes a los ataques *jamming* aleatorio, y los 3 casos correspondientes a los ataques *jamming* reactivo. En base a estos experimentos se ha realizado un análisis de los resultados obtenidos en los modelos GGM y GLGM con respecto a los datos de referencia. Para no extender el Capítulo, en este apartado sólo se representan los resultados correspondientes a la incidencia del segundo escenario de ataque, con el nodo atacante en el centro de la red de sensores inalámbricos. El resto de los resultados experimentales obtenidos para el primer y tercer escenario, se han representado en el Apéndice II y III.

En primer lugar, para el modelo GGM, se presentan en la Figura 6.20 los resultados pronosticados a corto plazo del número de nodos afectados por los ataques *jamming* aleatorio y reactivo. La Figura 6.20 (a) representa los datos tomados a los 50 segundos, y la Figura 6.20 (a) los datos tomados a los 60 segundos respectivamente. En ambas figuras, el valor medio de la incidencia pronosticada o número de nodos afectados en el instante t , está representado por el histograma gris, mientras que la incidencia dada por los datos de referencia se representa por un guion rojo horizontal. Las líneas verticales negras representan los límites superior e inferior correspondientes a los intervalos de confianza del 95 % de la incidencia pronosticada.

La Figura 6.20 (a) muestra los resultados de la estimación realizada por GGM, coincidiendo con el fin del periodo de calibración o etapa temprana de ataque considerada. De forma general, los resultados muestran un ajuste del modelo razonablemente bueno entre la incidencia pronosticada y los datos de referencia. De manera similar, la Figura 6.20 (b) muestra los resultados de la predicción de la incidencia realizada por GGM tras 10 segundos del periodo de calibración del ataque, mediante la extensión de la incertidumbre del sistema. En este caso, se observa cómo aparecen las primeras desviaciones entre la incidencia pronosticada y los datos reportados. De hecho, en el ejemplo presentado, se observa que para los protocolos

AODV y DSR se produce una rápida sobreestimación de la incidencia del ataque por parte del modelo, mientras que para MPH se mantiene en valores aceptables. Comentar que la sobreestimación de la incidencia tras 20 segundos de la etapa temprana del ataque, arroja en la mayoría de los casos, valores estimados que superan con creces al número de nodos existentes, esto es, $C_{\infty} \gg S_0$.

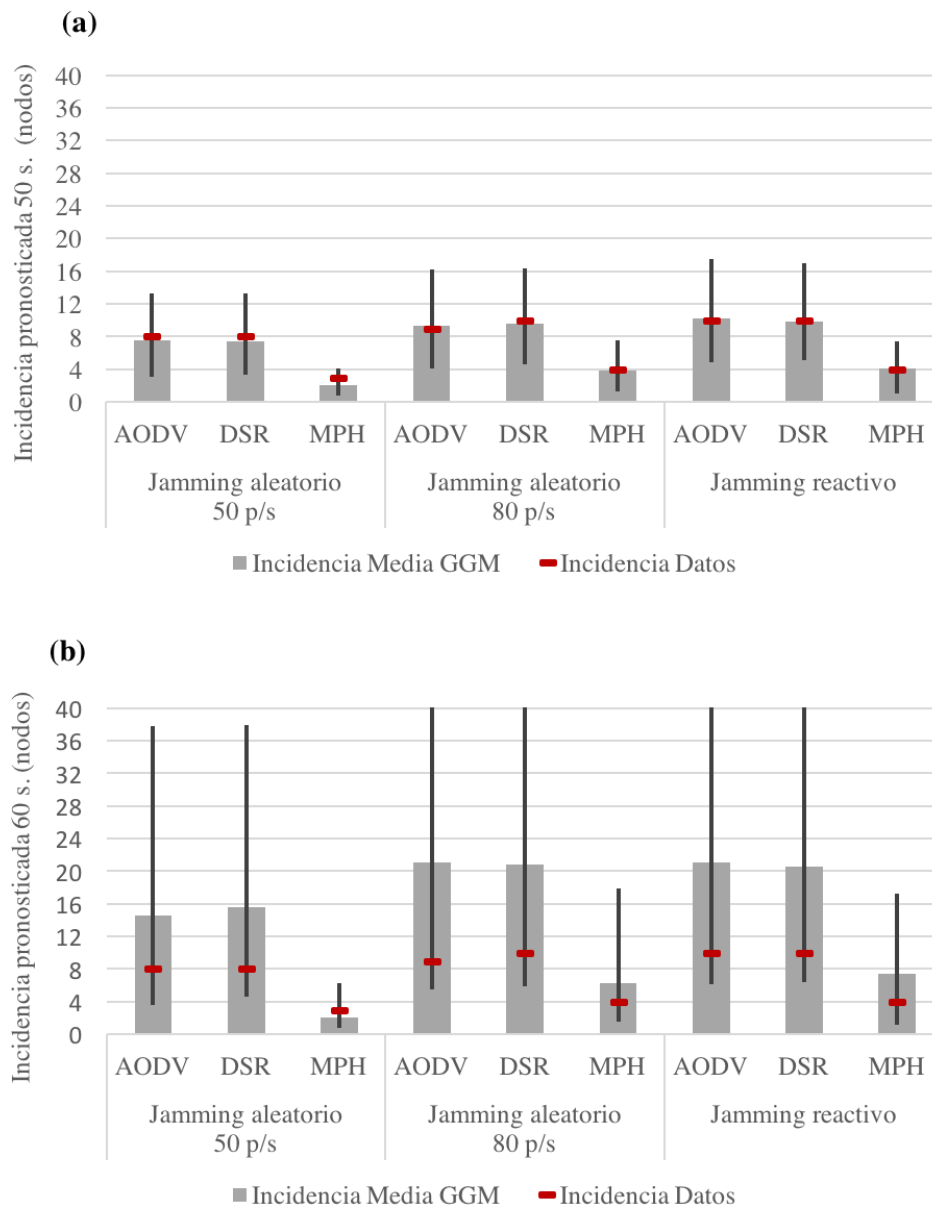


Figura 6.20. Comparativa de los resultados pronosticados por GGM de la evolución de nodos afectados o incidencia de los ataques *jamming* aleatorio y reactivo para el segundo escenario.

En segundo lugar, para el caso del modelo GLGM, en la Figura 6.21 se presentan los resultados del pronóstico a corto plazo obtenido experimentalmente y la evolución de la incidencia o número de nodos afectados tanto por los ataques de

jamming aleatorio como reactivo, correspondientes al segundo escenario de ataque. La Figura 6.21 (a) representa los datos experimentales tomados a los 50 segundos, (fin del periodo de calibración), y la Figura 6.21 (b) los datos tomados a los 60 segundos respectivamente. En ambas figuras, el valor medio de la incidencia pronosticada en el instante t , está representado por el histograma gris, mientras que la incidencia dada por los datos de referencia se representa por un guion rojo horizontal. Las líneas verticales negras representan los límites de los intervalos de confianza del 95 % de la incidencia.

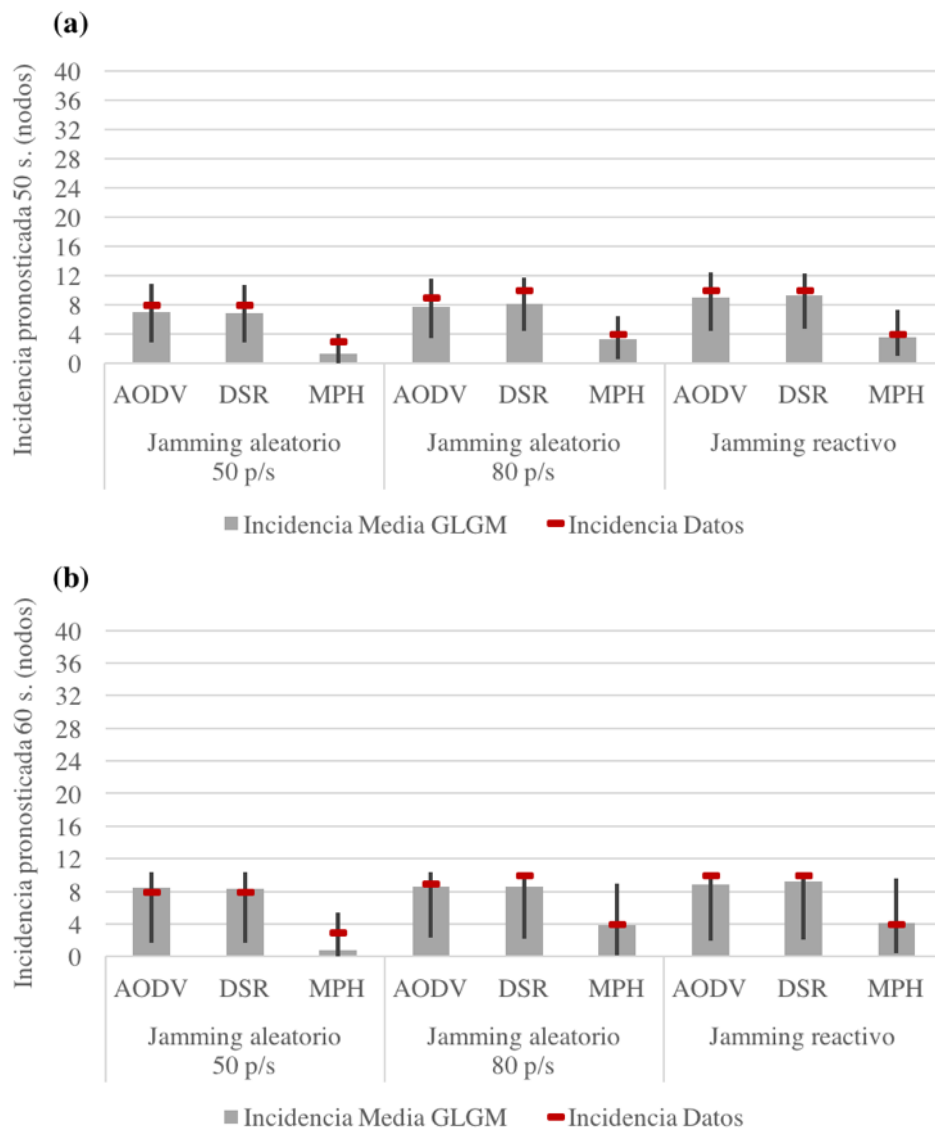


Figura 6.21. Comparativa de resultados pronosticados por GLGM de la evolución de nodos afectados por los ataques *jamming* aleatorio y reactivo para el segundo escenario, a los 50 s (a) y a los 60 s (b).

De forma general, los resultados de la Figura 6.21 (a) muestran un ajuste del modelo razonablemente bueno entre la incidencia pronosticada al final del periodo de

calibración y los datos de referencia. De manera similar, la Figura 6.21 (b) muestra los resultados de la predicción de la incidencia realizada por GLGM transcurridos 10 segundos desde el fin de la etapa temprana del ataque, mediante la extensión de la incertidumbre del sistema. En este caso, también se observa un ajuste del modelo razonablemente bueno entre la incidencia pronosticada y los datos reportados.

Para completar el conjunto de resultados de GLGM, en la Figura 6.22 se presentan los resultados pronosticados a medio plazo por el modelo GLGM y la evolución de la incidencia tanto por los ataques de *jamming* aleatorio como reactivo, correspondientes al segundo escenario de ataque. La Figura 6.22 (a) representa los datos experimentales tomados a los 70 segundos, y la Figura 6.22 (b) los datos tomados a los 80 segundos. En ambas figuras, el valor medio de la incidencia pronosticada en el instante t , está representado por el histograma gris, mientras que la incidencia dada por los datos de referencia se representa por un guion rojo horizontal. Las líneas verticales negras representan los límites de los intervalos de confianza del 95 % de la incidencia.

En la Figura 6.22 (a), muestra los resultados experimentales pronosticados por GLGM transcurridos 20 segundos del periodo de calibración, y superado, además el pico del ataque. Se observa ahora, que el ajuste del modelo en esta etapa proporciona unos resultados razonablemente buenos si comparamos la incidencia pronosticada y los datos de referencia. De manera similar, la Figura 6.21 (b) muestra los resultados experimentales de la predicción de la incidencia realizada por GLGM, transcurridos 30 segundos desde el fin de la etapa temprana del ataque. En este caso, también se observa un ajuste del modelo razonablemente bueno entre la incidencia pronosticada y los datos de referencia reportados. Es fácil comprobar que, para todos los tipos de ataques del escenario estudiado, el protocolo MPH parece mostrar una mejor resistencia frente al *jamming* que los protocolos AODV y DSR. Esto se observa el modelo ha pronosticado una mayor incidencia del ataque para los protocolos AODV y DSR que para el protocolo en MPH.

Como ya se indicó con anterioridad, la inclusión del parámetro K en el modelo GLGM, proporciona el un límite superior para el número total de nodos afectados, mejorando notablemente el pronóstico de dicha incidencia tras el pico del ataque, incluso mediante la extensión de la incertidumbre del sistema a lo largo del tiempo.

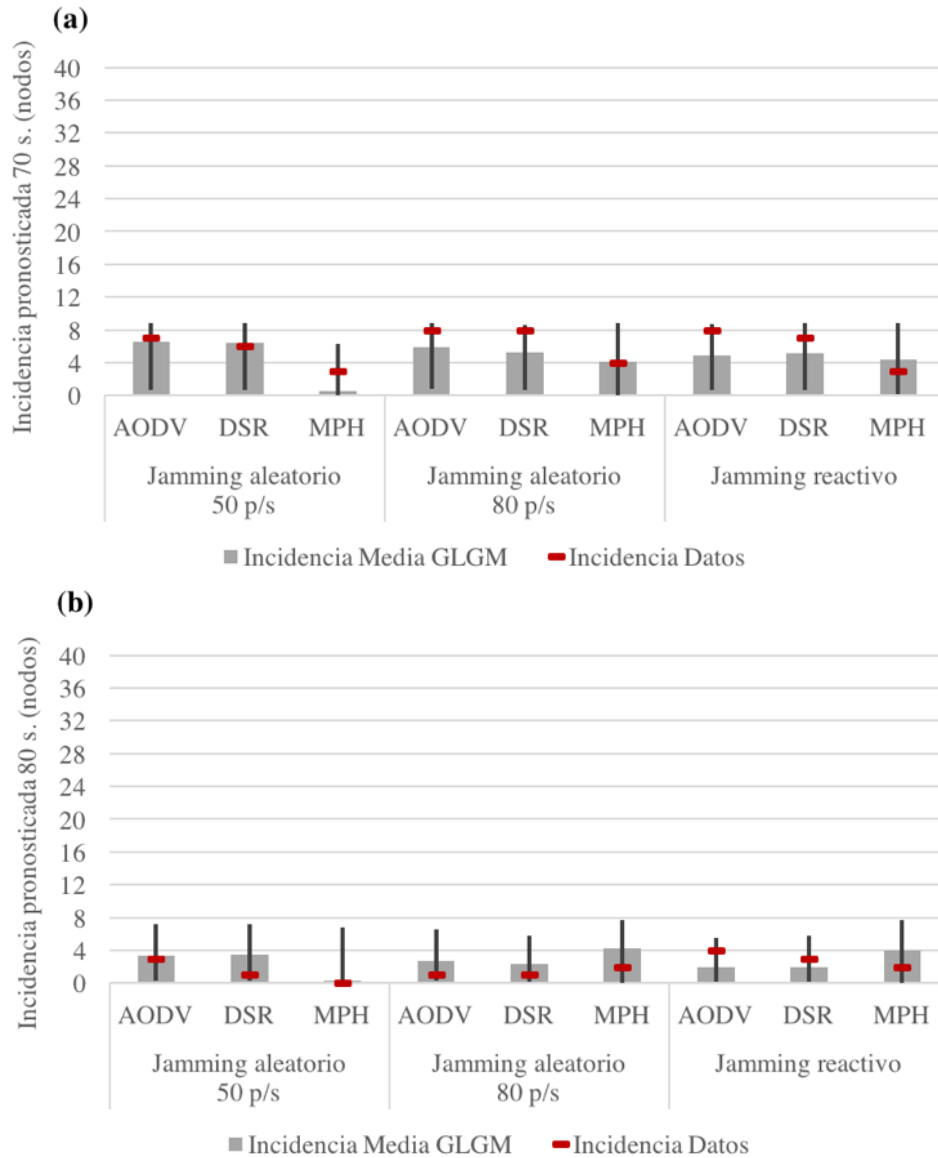


Figura 6.22. Comparativa de resultados pronosticados por GLGM de la evolución de nodos afectados por los ataques *jamming* aleatorio y reactivo para el segundo escenario, a los 70 s (a) y a los 80 s (b).

Por último, resaltar que, en general, los resultados obtenidos indican que los diferentes modelos epidemiológicos utilizados en el experimento han permitido determinar diferentes perfiles de crecimiento de las curvas características de los ataques *jamming*, incluso en un contexto de datos empíricos limitados, mostrando un ajuste razonablemente óptimo entre la incidencia pronosticada y los datos de referencia reportados para la mayoría de los escenarios de ataque.

6.4 Conclusiones

En el presente Capítulo, como contribución principal de esta Tesis, se ha realizado la validación de los modelos epidemiológicos propuestos mediante un estudio experimental exhaustivo. Para ello, se han utilizado los materiales y métodos descritos en el Capítulo 5, prestando especial atención a la importancia del conocimiento de los parámetros que caracterizan cada uno de los casos de ataque *jamming* aleatorio y reactivo objeto de estudio. La obtención de dichos parámetros característicos, han permitido además realizar un análisis, mediante la comparación de los resultados obtenidos con respecto a un conjunto de datos de referencia.

En el caso del modelo SIR determinista, se han estimado el parámetro β o tasa de contagio; el parámetro γ , que ha permitido analizar y conocer la persistencia del ataque y valorar su severidad; y el parámetro ν , con el que se han contabilizado los posibles nodos que pierdan totalmente su funcionalidad durante el ataque, lo que dota al modelo de una mayor aplicabilidad. Para el caso de los modelos fenomenológicos, de crecimiento generalizado y crecimiento logístico, los parámetros de interés obtenidos han sido la tasa de crecimiento intrínseca r , la desaceleración del factor de crecimiento p , y el tamaño final del ataque K . Los dos primeros parámetros, han permitido identificar cuán rápido se propaga el ataque entre los nodos sensores, mientras que el último, se ha utilizado como un indicativo de la severidad del ataque, permitiendo así un análisis y comparación posterior de cada uno de los ataques. Entre estos parámetros de interés se ha determinado el número reproductivo básico \mathcal{R}_0 que marca la diferencia entre un proceso epidémico, que propagará el ataque a través de la red, o un proceso no epidémico, en el que el ataque se extinguirá con rapidez. También se ha comprobado que el parámetro \mathcal{R}_0 puede utilizarse como un indicativo de la severidad del ataque.

Según los resultados obtenidos experimentalmente de las simulaciones, el menor valor obtenido para \mathcal{R}_0 es de 0.9967 (*jamming* aleatorio a 50 paquetes/segundo contra MPH, y tercer escenario de ataque), y un \mathcal{R}_0 máximo de 3.192 (*jamming* reactivo contra AODV, y segundo escenario de ataque). La media de \mathcal{R}_0 obtenida es de 1.617 para el conjunto de ataques y escenarios estudiados. Estos valores han permitido comparar la incidencia del conjunto de ataques *jamming* con brotes epidémicos conocidos.

CAPÍTULO

7

Conclusiones y trabajos futuros

En este último Capítulo de la Tesis, se exponen las principales conclusiones extraídas de esta investigación en la que se ha presentado un enfoque epidemiológico de propagación de enfermedades, para la caracterización y análisis de los ataques tipo *jamming* en redes de sensores inalámbricos. Este enfoque se ha desarrollado en base a la idea de que, en una red de sensores inalámbricos un ciberataque cuyo medio de transmisión principal es el aire, se propagará entre los nodos de la red del mismo modo en el que lo haría un virus de transmisión aérea entre los individuos en una población.

Desde esta perspectiva *bioinspirada*, se han realizado una serie de experimentos para estudiar cómo estos ataques pueden afectar a la funcionalidad de los nodos que conforman una red de sensores inalámbricos, independientemente de la complejidad y capacidad de procesamiento de dichos nodos. Los resultados obtenidos, han proporcionado la base para predecir la dinámica de propagación del ataque a través del tiempo en una población de nodos definida.

A su vez, en este Capítulo se destacan las principales contribuciones y aportaciones realizadas en el marco de esta Tesis, para la caracterización y análisis de los ataques tipo *jamming* en redes de sensores inalámbricos.

7.1 Introducción

A lo largo de los diferentes Capítulos de esta Tesis se ha abordado, la aplicación de diferentes modelos epidemiológicos para la caracterización y análisis de ataques tipo *jamming* aleatorio y reactivo contra redes de sensores inalámbricos. Este enfoque epidemiológico se ha validado mediante una serie de experimentos sobre diferentes escenarios de ataque, siendo comparados los resultados experimentales con un conjunto de datos de referencia.

En general, los resultados obtenidos indican que los diferentes modelos epidemiológicos propuestos en esta Tesis han permitido determinar diferentes perfiles de crecimiento de las curvas características de los ataques *jamming*, incluso en un contexto de datos empíricos limitados, mostrando un ajuste razonablemente óptimo entre la incidencia pronosticada y los datos de referencia reportados para la mayoría de los escenarios de ataque.

Estos resultados han permitido la comparación de la incidencia del conjunto de ataques *jamming* con brotes epidémicos de enfermedades conocidas.

7.2 Conclusiones generales

La primera contribución general de esta Tesis, ha sido la revisión del estado actual del arte en cuanto a la tecnología de redes de sensores inalámbricos, proporcionando una visión general que incluye desde aspectos como los elementos hardware y software que componen estas redes, hasta las arquitecturas y protocolos sobre los que se sustenta, además de las aplicaciones actuales, los retos en su despliegue y sus perspectivas de evolución en el ámbito del Internet de las Cosas (*Internet of Things*, IoT).

En segundo lugar, se han abordado los aspectos principales relacionados con la Ciberseguridad en redes de sensores inalámbricos, aportando una visión de conjunto sobre las principales amenazas y ataques, así como de los mecanismos y sistemas de seguridad que habitualmente se implementan en este tipo de redes. En especial, se ha revisado en mayor profundidad el ciberataque de interferencia conocido también como *jamming*, siendo éste la base para la investigación presentada en esta Tesis.

Otra de las contribuciones destacables ha sido el estudio de los modelos matemáticos más relevantes utilizados en epidemiología. Dentro de este amplio campo de estudio, en primer lugar, se comenzó con la descripción del grupo de los modelos denominados *mecanicistas*, definiendo primeramente conceptos básicos propios de la epidemiología. En este sentido, se definieron conceptos que lamentablemente hoy en día están muy presentes en nuestras vidas, tales como el número reproductivo básico \mathcal{R}_0 , la incidencia acumulada, el número de susceptibles, infectados o recuperados, la tasa de mortalidad, o la tasa de contagio, entre otros. Dentro de estos modelos *mecanicistas*, se hizo especial énfasis en la formulación matemática del modelo básico *Susceptible, Infectado, Recuperado* (SIR). Este modelo, es considerado como modelo básico en epidemiología, pero a la vez realmente versátil, en el estudio de enfermedades infecciosas, y resulta el modelo base para el desarrollo de modelos más complejos. De igual forma, en esta Tesis se han revisado, modelos más complejos que derivan del modelo SIR, aunque no de forma tan exhaustiva, donde se han incluido modelos que contemplan la vacunación de los individuos de la población, la cuarentena o la existencia de múltiples cepas de un mismo patógeno.

Por otra parte, también se incluyeron en este estudio los modelos epidemiológicos, denominados modelos *fenomenológicos*, los cuales suelen utilizarse para realizar predicciones a corto y medio plazo de la evolución de una enfermedad dentro de una población, tomando como referencia series de datos empíricos u observaciones al inicio de la epidemia. En este caso, se seleccionaron para el estudio el modelo de crecimiento exponencial (*Generalized Growth Model*, GGM) y el modelo de crecimiento logístico generalizado (*Generalized Logistic Growth Model*, GLGM).

Señalar que, el desarrollo de los modelos epidemiológico objeto de esta Tesis se ha centrado en aquellos modelos que estudian las denominadas enfermedades infecciosas, ya que sus características de propagación (pueden ser transmitidas de un individuo a otro dentro de una determinada población, ya sea de forma directa o indirecta), hacen que la proximidad de un individuo sano a otro individuo infectado suponga un aumento significativo del riesgo o probabilidad de resultar también infectado. Este concepto de transmisión por proximidad en ausencia de contacto, se ajusta al modelo de comunicación inalámbrica utilizado en las redes a estudio.

7.3 Conclusiones particulares

En cuanto a las aportaciones relacionadas con la implementación del proceso de validación de los modelos propuestos en esta Tesis, en primer lugar, se han presentado los materiales y métodos que conforman el entorno de simulación para llevar a cabo de forma experimental, la caracterización y análisis del comportamiento del ataque *jamming* en diferentes escenarios. Para ello, se procedió a la selección de los modelos epidemiológicos adecuados, prestado especial atención a la importancia del conocimiento de los parámetros que los definen. En este sentido, se ha elegido, por una parte, el modelo *mecanicista* básico *Susceptible, Infectado, Recuperado* (SIR), al que se le ha añadido el grupo de los nodos *Caídos* (*Dropped*), conformando un modelo SIRD. Por otra parte, y con objeto de aportar valor añadido a esta Tesis, también se ha tratado la predicción de la propagación de ataques *jamming*, para lo que se han seleccionado los modelos *fenomenológicos* de crecimiento exponencial (*Generalized Growth Model*, GGM) y de crecimiento logístico generalizado (*Generalized Logistic Growth Model*, GLGM). Éstos últimos, utilizan series de datos empíricos u observaciones en las etapas iniciales de una enfermedad para realizar predicciones o pronósticos a corto y medio plazo de la evolución de ésta dentro de una población.

En segundo lugar, como parte de los materiales y métodos utilizados, se ha realizado una descripción detallada del modelo de red de sensores inalámbricos a estudio, definiendo aspectos como la estructura de la red sobre la que se propagará el ataque *jamming* y los protocolos utilizados. También se ha definido aquí el comportamiento esperado de los nodos desde el punto de vista epidemiológico, enfatizando en los efectos que el ataque produce sobre estos nodos, y cómo estos van cambiando su estado frente al ataque, tal y como los individuos de una población lo hacen con respecto a una enfermedad infecciosa.

Finalmente, para abordar la fase experimental se necesitaba un conjunto de datos empíricos que ofreciesen la posibilidad de comparar de forma adecuada los datos obtenidos experimentalmente con dichos datos de referencia. En este caso, se ha seleccionado un conjunto de datos de referencia obtenidos por simulación, correspondientes a resultados publicados relativos a la ejecución de diferentes tipos de ataques *jamming* contra una red de sensores inalámbricos en varios escenarios de interés.

Con estos materiales y métodos definidos, se dispuso del marco de trabajo adecuado para realizar la validación de los modelos epidemiológicos propuestos mediante un estudio experimental, como contribución principal de la investigación llevada a cabo en esta Tesis. Para ello, se realizaron dos baterías de experimentos, la primera utilizando el modelo *mecanicista* antes definido, y la segunda batería utilizando los modelos *fenomenológicos* también descritos.

En ambos casos, y como otra de las contribuciones de interés, se desarrollaron y programaron en MATLAB los métodos necesarios para el cálculo y estimación de los parámetros que definían cada modelo epidémico, basando tales estimaciones en el conocimiento de series de datos empíricos de referencia. De aquí se obtuvieron los valores estimados, así como los intervalos de confianza para cada uno de dichos parámetros de interés

La primera batería de experimentos, se centró en el estudio de la propagación del *jamming* aleatorio y reactivo en tres escenarios de ataque, usando el modelo *Susceptible, Infectado, Recuperado, Caído* (SIRD). Esta batería de experimentos se dividió, a su vez, en dos subconjuntos. En el primero se abordó la caracterización y análisis del ataque de forma retrospectiva, esto es, con el conocimiento a posteriori de cómo había evolucionado el ataque a lo largo del tiempo. Mientras que el segundo conjunto de experimentos se enfocó en el estudio de la propagación del ataque desde el punto de vista predictivo, tomando como referencia sólo la etapa temprana del ataque.

Por otra parte, y como otra de las contribuciones de interés, se realizó una segunda batería de experimentos se centró en el estudio de la propagación del *jamming* aleatorio y reactivo ataque, desde el punto de vista predictivo, pero utilizando en este caso los modelos *fenomenológicos* de crecimiento exponencial (*Generalized Growth Model*, GGM) y de crecimiento logístico generalizado (*Generalized Logistic Growth Model*, GLGM). Para ello, se estudiaron los tres escenarios de ataque tomando como referencia los datos empíricos u observaciones en las etapas iniciales de dichos ataques, para realizar predicciones a corto y medio plazo de su evolución.

De hecho, y hasta donde se ha podido constatar, la aplicación de modelos de propagación de epidemias para el análisis predictivo de la propagación de ataques *jamming* en redes de sensores inalámbricos, no se había planteado anteriormente, por lo tanto, la investigación desarrollada en este sentido en el marco de esta Tesis puede considerarse como especialmente relevante e innovadora.

Como una de las contribuciones más interesantes, cabe destacar que los resultados obtenidos en las dos baterías de experimentos, han corroborado que los modelos epidemiológicos propuestos son capaces de caracterizar la dinámica de propagación del ataque *jamming* sobre la red inalámbrica con una precisión óptima, cumpliendo totalmente con las expectativas deseadas. Además, éstos mismos modelos epidemiológicos, han proporcionado valores de incidencia al final del ataque acordes con los datos de referencia, lo que ha permitido el cálculo de número reproductivo básico \mathcal{R}_0 , y la comparación de dicha incidencia, con la incidencia producida por brotes epidémicos conocidos. Este hecho, supone otra aportación de destacable, ya que la elección del número reproductivo básico \mathcal{R}_0 , como parámetro fundamental para caracterizar los efectos de la propagación del ataque *jamming* sobre la red inalámbrica, también ha permitido analizar la robustez o resiliencia de la propia red dependiendo del protocolo de enrutamiento utilizado. Esta cuestión resulta muy importante de cara a mantener la red inalámbrica operativa en aplicaciones de infraestructuras críticas, procesos industriales, entornos medioambientales y otras aplicaciones basadas en la recopilación de datos en tiempo real.

7.4 Publicaciones relacionadas con la Tesis

Las publicaciones que han surgido a raíz del desarrollo de la Tesis, cubren dos campos de estudio bien diferenciados. Por una parte, se han publicado una serie de artículos basado en sistemas *bioinspirados*, relacionados con la Ciberseguridad en redes de sensores inalámbricos propiamente dicha, donde se han tratado los ataques *jamming* contra este tipo de redes como brotes epidémicos. En este mismo grupo de artículos, se incluye un modelo para detección de intrusos basado en la teoría de juegos evolutiva. Por otra parte, y motivado por la investigación en el campo de la epidemiología, se ha publicado un trabajo de investigación donde se aborda la propagación de la segunda ola de la pandemia de COVID-19 en el territorio español. A continuación, se presenta un resumen de los trabajos de investigación publicados:

- M. López, A. Peinado, A. Ortiz. *Characterizing two outbreak waves of COVID-19 in Spain using phenomenological epidemic modelling*. PLOS ONE, June 24th, 2021.
- M. López, A. Peinado, A. Ortiz. *An extensive validation of a SIR epidemic model to study the propagation of jamming attacks against IoT wireless networks*. Computer Networks, Volume 165, 24 December 2019, Elsevier B.V.
- M. López, A. Peinado, A. Ortiz. *Validation of a SIR Epidemic Model for the Propagation of Jamming Attacks in Wireless Sensor Networks*. M. López, A. Peinado, A. Ortiz. RECSI XV, Granada, 3-5 octubre 2018, Sesión 5, IoT y SmartGrid, ISBN: 978-84-09-02463-6.
- M. López. *On the Effectiveness of Intrusion Detection Strategies for Wireless Sensor Networks: An Evolutionary Game Approach*. Ad Hoc & Sensor Wireless Networks, Vol. 35, 2017, pp. 25–40. Old City Publishing, Inc. Philadelphia, USA.
- A M. López, A. Peinado, A. Ortiz. *A SEIS Model for Propagation of Random Jamming Attacks in Wireless Sensor Networks*. International Joint Conference SOCO'16-CISIS'16-ICEUTE'16. San Sebastián, octubre 2016.
- M. López, A. Peinado, A. Ortiz. *Modelo epidemiológico para la propagación del jamming aleatorio en redes de sensores inalámbricos*. XIV Reunión Española sobre Criptología y Seguridad de la Información, RECSI 2016. Octubre 2016.
- M. López, A. Peinado, A. Ortiz. *Modelo epidemiológico para el estudio de los ataques tipo jamming en redes de sensores inalámbricos*. JNIC2016, Sesión 1: Seguridad Industrial, Infraestructuras Críticas. Granada, junio 2016.

7.5 Trabajos futuros

Además de las publicaciones y trabajos publicados antes mencionados, el desarrollo de la presente Tesis ha abierto el camino hacia diferentes líneas de investigación que pueden ampliar o continuar la propuesta *bioinspirada* de utilización de modelos epidemiológicos para la caracterización y análisis de ataques *jamming* de diferente naturaleza en redes de sensores inalámbricos.

- Con respecto al uso de modelos epidemiológicos *mecanicistas*, se propone abordar el uso de modelos como el *Susceptible, Infectado, Recuperado* (SIR) desde una perspectiva estocástica. Los procesos estocásticos son un concepto matemático utilizado para tratar variables sujetas a influencias o efectos aleatorios que varían con el tiempo. Este tratamiento resulta de especial interés en epidemiología cuando el número de individuos susceptibles e infectados dentro de la población es pequeño y/o cuando el ambiente afecta la variabilidad en el resultado de las tasas de transmisión y recuperación de la epidemia.
- Con respecto al uso de modelos *fenomenológicos* de propagación de epidemias para realizar análisis predictivos de la propagación de ataques *jamming* en redes de sensores inalámbricos, como ya se indicó anteriormente, en esta Tesis se ha propuesto por primera vez el uso de este tipo de modelos, lo que abre el camino a investigar modelos más complejos en este campo. Esto permitiría desarrollar sistemas de detección de ataques a redes inalámbricas basados en el análisis de la incidencia en la fase temprana de éstos.
- Con respecto a la dependencia de la incidencia del ataque del número reproductivo básico \mathcal{R}_0 , se propone el diseño seguro de redes mediante el estudio de los parámetros que lo conforma. Por ejemplo, conocido que la tasa de contagio β se compone de un parámetro que representa la probabilidad de existencia de un enlace en el nivel físico, y de otro parámetro que representa la probabilidad de que el ataque sea efectivo dado el contacto entre un nodo susceptible y un nodo afectado, se puede establecer la relación $\mathcal{R}_0 = 1$ para estimar el radio mínimo necesario para mantener la comunicación efectiva entre nodos, pero manteniendo, a su vez, la distancia de seguridad o radio de alcance suficiente entre nodos, para que en caso de ataque éste no se propague con rapidez por la red.
- Por último, en relación a la disponibilidad de datos de referencia para desarrollar experimentos futuros, sería interesante poder contar con plataformas de pruebas online o colaborativas, en las que desplegar (de forma real o virtual) redes de sensores inalámbricos sobre las que ejecutar diferentes tipos de ataques *jamming*, con diferentes arquitecturas, protocolos

y teniendo en cuenta, por ejemplo, aspectos como la movilidad de los nodos. De este modo, se dispondría de un gran número de patrones de ataque que permitirían, nuevas líneas de investigación, como, por ejemplo, el desarrollo de sistemas de detección de intrusos para redes de sensores inalámbricos basados en patrones de comportamiento capaces de detectar un aumento anómalo de nodos inalcanzables en la red, o incluso el análisis de parámetros tales como el número de paquetes retransmitidos, el aumento del consumo de energía de los nodos, o el aumento de colisiones en la capa de red de acceso al medio, entre otros.

7.6 Conclusiones

En este Capítulo final de la Tesis, se han expuesto las principales conclusiones extraídas de esta investigación en la que se ha presentado un enfoque epidemiológico de propagación de enfermedades, para la caracterización y análisis de los ataques tipo *jamming*.

Este enfoque de análisis de los ciberataques se enmarca en el concepto de sistemas *bioinspirados*, los cuales se centran comprender los fundamentos de ciertos sistemas biológicos, captando su comportamiento dinámico para ser posteriormente aplicado a sistemas no biológicos, ofreciendo un campo de estudio realmente interesante y, por su naturaleza, aplicable a las redes de sensores inalámbricos.

Con todo lo expuesto, se puede considerar que ha quedado cubierto el objetivo principal de esta Tesis Doctoral, que no era otro que diseñar, desarrollar y proponer nuevas metodologías y modelos que permitan mejorar la Ciberseguridad de las redes de sensores inalámbricos y reducir así el riesgo asociado a un ciberataque en este tipo de redes, bien reduciendo el factor de probabilidad de riesgo, reduciendo el factor de impacto, o ambos a la vez.

APÉNDICE

I

**Desarrollo de la Matriz de Siguiete Generación
(*Next Generation Matrix*) para el cálculo del
número reproductivo básico \mathcal{R}_0**

En el Capítulo 4 se discutieron métodos para el estudio de la estabilidad de los puntos de Equilibrio Libre de Enfermedad (*Disease Free Equilibrium*, DFE) y Equilibrio Endémico (*Endemic Equilibrium*, EE), basados en funciones de Poincaré-Lyapunov, o en la aplicación de técnicas de linealización mediante operadores *Jacobianos* [125]. En este apartado se presente un método alternativo para el estudio de la estabilidad basado en el cálculo de \mathcal{R}_0 . Este método, propuesto por P. Van Den Driessche y J. Watmough [115], hace uso del operador denominado de *Próxima Generación* (*Next-Generatiom Operator*) sugerido por Diekmann, Heesterbeek, y Metz [114]. Este método es aplicable a modelos epidémicos deterministas compartimentales de dimensión finita, descritos mediante sistema de ecuaciones diferenciales ordinarias, tal y como es el caso del modelo propuesto.

En primer lugar, la dinámica del sistema epidémico se reescribe separando, las variables de estado de los flujos entrantes relacionados con el proceso infeccioso, dando como resultado un sistema dinámico compartimental alternativo cuya dinámica se describe por la función $\dot{x} = f_i(x)$ con $x = (x_1, x_2, \dots, x_p, x_{p+1}, \dots, x_n)^T$, donde x_p, x_{p+1}, \dots, x_n representa la población de nuevos infectados. Realizando la siguiente partición en $f: \mathbb{R}^n \rightarrow \mathbb{R}^n$ se obtiene que [115].

$$\dot{x} = \frac{dx}{dt} = \mathcal{F}_i(x) + \mathcal{V}_i(x) = \mathcal{F}_i(x) + (\mathcal{V}_i^+ - \mathcal{V}_i^-)(x) \quad \text{A.1}$$

donde \mathcal{F}_i , representa la tasa a la que los nuevos infectados pasan al compartimento i , mientras que $\mathcal{V}_i^+, \mathcal{V}_i^-$, representan otros flujos de entrada y salida, respectivamente, hacia o desde el i -ésimo compartimento, siendo todas ellas funciones no negativas. Si x_0 es un equilibrio libre de enfermedad DFE, entonces las derivadas $D\mathcal{F}(x_0)$, y $D\mathcal{V}(x_0)$, pueden particionarse como [115]

$$D\mathcal{F}(x_0) = \begin{pmatrix} F & 0 \\ 0 & 0 \end{pmatrix}, D\mathcal{V}(x_0) = \begin{pmatrix} V & 0 \\ J_3 & J_4 \end{pmatrix} \quad \text{A.2}$$

donde F y V son matrices cuadradas de dimensión $m \times m$, cuyos términos vienen dados por las siguientes derivadas parciales

$$F = \left[\frac{\partial \mathcal{F}_i}{\partial x_j}(x_0) \right], V = \left[\frac{\partial \mathcal{V}_i}{\partial x_j}(x_0) \right], \quad 1 \leq i, j \leq m \quad \text{A.3}$$

siendo la matriz F no es negativa, y V una matriz no singular siendo todos los valores propios de J_4 reales y positivos. Si la población permanece cerca del DFE, esto es, si la introducción de unos pocos individuos infecciosos no da como resultado una epidemia, entonces la población volverá al equilibrio libre de enfermedad DFE de acuerdo con el sistema linealizado dado por $\dot{x} = Df(x_0)(x - x_0)$, donde $Df(x_0)$ es la matriz *Jacobiana* $\partial f_i / \partial x_i$ evaluada en el DFE, x_0 .

El número reproductivo básico \mathcal{R}_0 se obtiene evaluando el equilibrio DFE en el sistema linealizado $\dot{x} = -D\mathcal{V}(x_0)(x - x_0)$, siendo éste un equilibrio local asintóticamente estable en este sistema linealizado. El objetivo principal es establecer la

relación entre el número reproductivo básico \mathcal{R}_0 y el valor de la parte real del valor propio dominante del producto FV^{-1} , denominado operador Matriz de Próxima Generación (*Next-Generatiom Matrix*). Esta relación se expresa como $\mathcal{R}_0 = \rho(FV^{-1})$ donde ρ es –en valor absoluto– el máximo de los valores propios o radio espectral de la matriz FV^{-1} [115]. Para determinar los valores que conforman el producto FV^{-1} y desarrollar una definición para \mathcal{R}_0 , se considera una población en el estado DFE, en la que se introduce un individuo infectado en el compartimento k . Los elementos (j, k) de la matriz V^{-1} representan el tiempo promedio durante el que este individuo permanece en compartimento j , asumiendo que la población permanece cerca del DFE y la ausencia de reinfección. Por otra parte, los elementos (i, j) de la matriz F representa la tasa a la que los individuos infectados en el compartimento j producen nuevas infecciones en el compartimento i . Por lo tanto, los elementos (i, k) del producto FV^{-1} representan el número esperado de nuevas infecciones en el compartimento i producidas por el individuo infectado originalmente introducido en el compartimento k . En estas condiciones, el equilibrio libre de enfermedad DFE en x_0 , es un equilibrio local asintóticamente estable en este sistema linealizado si todos los valores propios de la matriz $Df(x_0)$ tienen partes reales negativas. Si por el contrario algún valor propio de $Df(x_0)$ tiene una parte real positiva, entonces se trata de un equilibrio local asintóticamente e inestable [115].

Para determinar los valores que conforman el producto FV^{-1} y desarrollar una definición para \mathcal{R}_0 en el caso del modelo de propagación de ataques *jamming* propuesto, se asume que la población total de nodos es constante pudiendo focalizar el estudio del equilibrio utilizando las ecuaciones 4.5 y 4.6 del modelo epidemiológico SIR, para los nodos susceptibles (S) e infectados (I) respectivamente. Siguiendo el proceso indicado en el párrafo anterior, claramente, la partición del sistema linealizado viene dada por la ecuación

$$\dot{x}(S, I) = \mathcal{F}(S, I) + \mathcal{V}^+(S, I) - \mathcal{V}^-(S, I) \quad \text{A.4}$$

donde $\mathcal{F}(S, I) = (0, \beta SI)$, $\mathcal{V}^+(S, I) = (0, 0)$ y $\mathcal{V}^-(S, I) = (-\beta SI, -(\gamma + \mu)I)$. Al evaluar el sistema 4.9 en punto próximo al equilibrio DFE $(S^*, 0)$, para $S^* \geq 0$, se obtiene que

$$F = \left[\frac{\partial \mathcal{F}}{\partial S} (S^*, 0) \right] = \beta S^*, \quad V = \left[\frac{\partial \mathcal{V}}{\partial I} (S^*, 0) \right] = -(\gamma + \mu) \quad \text{A.5}$$

siendo

$$\mathcal{R}_0 = \rho(FV^{-1}) = \frac{\beta S^*}{\gamma + \mu} \quad \text{A.6}$$

De esta expresión, se deduce que para el modelo propuesto en el que solo existe un compartimento de infectados, \mathcal{R}_0 es el producto de la tasa de infección por el número de nodos sanos en el DFE, dividido entre el tiempo medio en el que los nodos afectados permanecen en este estado, o duración media de la infección. Con esta definición, se concluye que:

1. Si $\mathcal{R}_0 < 1$, entonces el equilibrio libre de enfermedad DFE $(S^*, 0)$ es asintóticamente estable,
2. Si $\mathcal{R}_0 > 1$, entonces el equilibrio libre de enfermedad DFE $(S^*, 0)$ es inestable

Desde un punto de vista matemático, el número reproductivo básico \mathcal{R}_0 se define como el número de nuevas infecciones producidas por un individuo infeccioso típico en una población que se encuentra en el estado estacionario libre de enfermedad (DFE) [114]. Si $\mathcal{R}_0 < 1$, cada nodo afectado producirá menos de un nuevo nodo afectado en el transcurso del periodo que dure el ataque, por lo que éste no progresará a través de la población. Por el contrario, si $\mathcal{R}_0 > 1$, cada nodo afectado producirá, en promedio, más de una infección nueva, y el ataque puede propagarse en la red de sensores.

Para una población N lo suficientemente grande, y teniendo en cuenta que al inicio de la infección $I_0 \ll N$, y $S_0 = N - I_0$, se puede asumir que $S^* = S_0 \approx N$, obteniendo, por tanto, un valor para el número reproductivo básico $\mathcal{R}_0 = \beta N / (\gamma + \mu)$, siendo equivalente al valor obtenido en el análisis del modelo SIR realizado en el capítulo anterior.

APÉNDICE

II

Relación de tablas y datos relevantes obtenidos de los diferentes experimentos

En el desarrollo de esta investigación, el conjunto de experimentos realizados ha generado una serie de datos correspondientes a un total de 108 casos de estudio para los diferentes modelos epidemiológicos y escenarios de ataque. En el este Apéndice se agrupan las tablas de datos, donde pueden observarse los resultados más relevantes obtenidos en los diferentes experimentos. Estos resultados experimentales son suficientemente representativos como para determinar la validez de cada uno de los modelos epidemiológicos propuestos. En cada uno de los siguientes apartados, se indica para cada uno de dichos modelos epidemiológicos, el caso de estudio y escenario objeto del experimento.

A.II.1 Tablas de datos de referencia para el primer escenario de ataque, donde el nodo atacante está próximo al nodo coordinador de la red de sensores inalámbricos.

AODV							DSR							MPH						
t(s)	I(t)	C(t)	S(t)	R(t)	D(t)	A(t)	t(s)	I(t)	C(t)	S(t)	R(t)	D(t)	A(t)	t(s)	I(t)	C(t)	S(t)	R(t)	D(t)	A(t)
0	1	0	48	0	0	48	0	1	0	48	0	0	48	0	1	0	48	0	0	48
10	5	5	43	0	0	43	10	4	4	44	0	0	44	10	4	4	44	0	0	44
20	1	6	42	5	0	47	20	0	4	44	4	0	48	20	0	4	44	4	0	48
30	1	7	41	6	0	47	30	0	4	44	4	0	48	30	0	4	44	4	0	48
40	2	9	39	7	0	46	40	2	6	42	4	0	46	40	2	6	42	4	0	46
50	7	16	32	9	0	41	50	5	11	37	6	0	43	50	2	8	40	6	0	46
60	7	23	25	16	0	41	60	5	16	32	11	0	43	60	2	10	38	8	0	46
70	7	30	18	23	0	41	70	5	21	27	16	0	43	70	3	13	35	10	0	45
80	2	32	16	30	0	46	80	1	22	26	21	0	47	80	0	13	35	13	0	48
90	1	33	15	32	0	47	90	1	23	25	22	0	47	90	0	13	35	13	0	48
100	0	33	15	33	0	48	100	0	23	25	23	0	48	100	0	13	35	13	0	48
110	0	33	15	33	0	48	110	0	23	25	23	0	48	110	0	13	35	13	0	48
120	0	33	15	33	0	48	120	0	23	25	23	0	48	120	0	13	35	13	0	48
130	0	33	15	33	0	48	130	0	23	25	23	0	48	130	0	13	35	13	0	48
140	0	33	15	33	0	48	140	0	23	25	23	0	48	140	0	13	35	13	0	48
150	0	33	15	33	0	48	150	0	23	25	23	0	48	150	0	13	35	13	0	48
160	0	33	15	33	0	48	160	0	23	25	23	0	48	160	0	13	35	13	0	48
170	0	33	15	33	0	48	170	0	23	25	23	0	48	170	0	13	35	13	0	48
180	0	33	15	33	0	48	180	0	23	25	23	0	48	180	0	13	35	13	0	48

Tabla A.II.1.1. Datos de referencia *jamming* aleatorio 50 paquetes/segundo.

AODV							DSR							MPH						
t(s)	I(t)	C(t)	S(t)	R(t)	D(t)	A(t)	t(s)	I(t)	C(t)	S(t)	R(t)	D(t)	A(t)	t(s)	I(t)	C(t)	S(t)	R(t)	D(t)	A(t)
0	1	0	48	0	0	48	0	1	0	48	0	0	48	0	1	0	48	0	0	48
10	4	4	44	0	0	44	10	5	5	43	0	0	43	10	4	4	44	0	0	44
20	0	4	44	4	0	48	20	1	6	42	5	0	47	20	1	5	43	4	0	47
30	1	5	43	4	0	47	30	0	6	42	6	0	48	30	0	5	43	5	0	48
40	1	6	42	5	0	47	40	3	9	39	6	0	45	40	2	7	41	5	0	46
50	7	13	35	6	0	41	50	8	17	31	9	0	40	50	4	11	37	7	0	44
60	7	20	28	13	0	41	60	8	25	23	17	0	40	60	4	15	33	11	0	44
70	8	28	20	20	0	40	70	7	32	16	25	0	41	70	3	18	30	15	0	45
80	1	29	19	28	0	47	80	1	33	15	32	0	47	80	2	20	28	18	0	46
90	0	29	19	29	0	48	90	1	34	14	33	0	47	90	0	20	28	20	0	48
100	0	29	19	29	0	48	100	0	34	14	34	0	48	100	0	20	28	20	0	48
110	0	29	19	29	0	48	110	0	34	14	34	0	48	110	0	20	28	20	0	48
120	0	29	19	29	0	48	120	0	34	14	34	0	48	120	0	20	28	20	0	48
130	0	29	19	29	0	48	130	0	34	14	34	0	48	130	0	20	28	20	0	48
140	0	29	19	29	0	48	140	0	34	14	34	0	48	140	0	20	28	20	0	48
150	0	29	19	29	0	48	150	0	34	14	34	0	48	150	0	20	28	20	0	48
160	0	29	19	29	0	48	160	0	34	14	34	0	48	160	0	20	28	20	0	48
170	0	29	19	29	0	48	170	0	34	14	34	0	48	170	0	20	28	20	0	48
180	0	29	19	29	0	48	180	0	34	14	34	0	48	180	0	20	28	20	0	48

Tabla A.II.1.2. Datos de referencia *jamming* aleatorio 80 paquetes/segundo.

AODV							DSR						MPH							
t(s)	I(t)	C(t)	S(t)	R(t)	D(t)	A(t)	t(s)	I(t)	C(t)	S(t)	R(t)	D(t)	A(t)	t(s)	I(t)	C(t)	S(t)	R(t)	D(t)	A(t)
0	1	0	48	0	0	48	0	1	0	48	0	0	48	0	1	0	48	0	0	48
10	4	4	44	0	0	44	10	3	3	45	0	0	45	10	2	2	46	0	0	46
20	1	5	43	4	0	47	20	0	3	45	3	0	48	20	0	2	46	2	0	48
30	0	5	43	5	0	48	30	0	3	45	3	0	48	30	0	2	46	2	0	48
40	2	7	41	5	0	46	40	2	5	43	3	0	46	40	1	3	45	2	0	47
50	9	16	32	7	0	39	50	8	13	35	5	0	40	50	4	7	41	3	0	44
60	9	25	23	16	0	39	60	8	21	27	13	0	40	60	4	11	37	7	0	44
70	6	31	17	25	0	42	70	7	28	20	21	0	41	70	3	14	34	11	0	45
80	4	35	13	31	0	44	80	3	31	17	28	0	45	80	2	16	32	14	0	46
90	2	37	11	35	0	46	90	2	33	15	31	0	46	90	0	16	32	16	0	48
100	1	38	10	37	0	47	100	1	34	14	33	0	47	100	0	16	32	16	0	48
110	0	38	10	37	1	47	110	0	34	14	33	1	47	110	0	16	32	16	0	48
120	0	38	10	37	1	47	120	0	34	14	33	1	47	120	0	16	32	16	0	48
130	0	38	10	37	1	47	130	0	34	14	33	1	47	130	0	16	32	16	0	48
140	0	38	10	37	1	47	140	0	34	14	33	1	47	140	0	16	32	16	0	48
150	0	38	10	37	1	47	150	0	34	14	33	1	47	150	0	16	32	16	0	48
160	0	38	10	37	1	47	160	0	34	14	33	1	47	160	0	16	32	16	0	48
170	0	38	10	37	1	47	170	0	34	14	33	1	47	170	0	16	32	16	0	48
180	0	38	10	37	1	47	180	0	34	14	33	1	47	180	0	16	32	16	0	48

Tabla A.II.1.3. Datos de referencia jamming reactivo.

A.II.2 Tablas de datos de referencia para el segundo escenario de ataque, donde el nodo atacante está en el centro de la red de sensores inalámbricos.

AODV							DSR						MPH							
t(s)	I(t)	C(t)	S(t)	R(t)	D(t)	A(t)	t(s)	I(t)	C(t)	S(t)	R(t)	D(t)	A(t)	t(s)	I(t)	C(t)	S(t)	R(t)	D(t)	A(t)
0	1	0	48	0	0	48	0	1	0	48	0	0	48	0	1	0	48	0	0	48
10	4	4	44	0	0	44	10	4	4	44	0	0	44	10	4	4	44	0	0	44
20	1	5	43	4	0	47	20	1	5	43	4	0	47	20	0	4	44	4	0	48
30	1	6	42	5	0	47	30	0	5	43	5	0	48	30	0	4	44	4	0	48
40	4	10	38	6	0	44	40	4	9	39	5	0	44	40	2	6	42	4	0	46
50	8	18	30	10	0	40	50	8	17	31	9	0	40	50	3	9	39	6	0	45
60	8	26	22	18	0	40	60	8	25	23	17	0	40	60	3	12	36	9	0	45
70	7	33	15	26	0	41	70	6	31	17	25	0	42	70	3	15	33	12	0	45
80	3	36	12	33	0	45	80	1	32	16	31	0	47	80	0	15	33	15	0	48
90	1	37	11	36	0	47	90	1	33	15	32	0	47	90	0	15	33	15	0	48
100	0	37	11	36	1	47	100	0	33	15	33	0	48	100	0	15	33	15	0	48
110	0	37	11	36	1	47	110	0	33	15	33	0	48	110	0	15	33	15	0	48
120	0	37	11	36	1	47	120	0	33	15	33	0	48	120	0	15	33	15	0	48
130	0	37	11	36	1	47	130	0	33	15	33	0	48	130	0	15	33	15	0	48
140	0	37	11	36	1	47	140	0	33	15	33	0	48	140	0	15	33	15	0	48
150	0	37	11	36	1	47	150	0	33	15	33	0	48	150	0	15	33	15	0	48
160	0	37	11	36	1	47	160	0	33	15	33	0	48	160	0	15	33	15	0	48
170	0	37	11	36	1	47	170	0	33	15	33	0	48	170	0	15	33	15	0	48
180	0	37	11	36	1	47	180	0	33	15	33	0	48	180	0	15	33	15	0	48

Tabla A.II.2.1. Datos de referencia jamming aleatorio 50 paquetes/segundo.

AODV							DSR						MPH							
t(s)	I(t)	C(t)	S(t)	R(t)	D(t)	A(t)	t(s)	I(t)	C(t)	S(t)	R(t)	D(t)	A(t)	t(s)	I(t)	C(t)	S(t)	R(t)	D(t)	A(t)
0	1	0	48	0	0	48	0	1	0	48	0	0	48	0	1	0	48	0	0	48
10	5	5	43	0	0	43	10	5	5	43	0	0	43	10	3	3	45	0	0	45
20	0	5	43	5	0	48	20	1	6	42	5	0	47	20	1	4	44	3	0	47
30	0	5	43	5	0	48	30	1	7	41	6	0	47	30	0	4	44	4	0	48
40	5	10	38	5	0	43	40	5	12	36	7	0	43	40	2	6	42	4	0	46
50	9	19	29	10	0	39	50	10	22	26	12	0	38	50	4	10	38	6	0	44
60	9	28	20	19	0	39	60	10	32	16	22	0	38	60	4	14	34	10	0	44
70	8	36	12	28	0	40	70	8	40	8	32	0	40	70	4	18	30	14	0	44
80	1	37	11	36	0	47	80	1	41	7	40	0	47	80	2	20	28	18	0	46
90	1	38	10	37	0	47	90	1	42	6	41	0	47	90	0	20	28	20	0	48
100	0	38	10	38	0	48	100	0	42	6	42	0	48	100	0	20	28	20	0	48
110	0	38	10	38	0	48	110	0	42	6	42	0	48	110	0	20	28	20	0	48
120	0	38	10	38	0	48	120	0	42	6	42	0	48	120	0	20	28	20	0	48
130	0	38	10	38	0	48	130	0	42	6	42	0	48	130	0	20	28	20	0	48
140	0	38	10	38	0	48	140	0	42	6	42	0	48	140	0	20	28	20	0	48
150	0	38	10	38	0	48	150	0	42	6	42	0	48	150	0	20	28	20	0	48
160	0	38	10	38	0	48	160	0	42	6	42	0	48	160	0	20	28	20	0	48
170	0	38	10	38	0	48	170	0	42	6	42	0	48	170	0	20	28	20	0	48
180	0	38	10	38	0	48	180	0	42	6	42	0	48	180	0	20	28	20	0	48

Tabla A.II.2.2. Datos de referencia *jamming* aleatorio 80 paquetes/segundo.

AODV							DSR						MPH							
t(s)	I(t)	C(t)	S(t)	R(t)	D(t)	A(t)	t(s)	I(t)	C(t)	S(t)	R(t)	D(t)	A(t)	t(s)	I(t)	C(t)	S(t)	R(t)	D(t)	A(t)
0	1	0	48	0	0	48	0	1	0	48	0	0	48	0	1	0	48	0	0	48
10	4	4	44	0	0	44	10	3	3	45	0	0	45	10	2	2	46	0	0	46
20	1	5	43	4	0	47	20	0	3	45	3	0	48	20	0	2	46	2	0	48
30	0	5	43	5	0	48	30	0	3	45	3	0	48	30	0	2	46	2	0	48
40	7	12	36	5	0	41	40	7	10	38	3	0	41	40	3	5	43	2	0	45
50	10	22	26	12	0	38	50	10	20	28	10	0	38	50	4	9	39	5	0	44
60	10	32	16	22	0	38	60	10	30	18	20	0	38	60	4	13	35	9	0	44
70	8	40	8	32	0	40	70	7	37	11	30	0	41	70	3	16	32	13	0	45
80	4	44	4	40	0	44	80	3	40	8	37	0	45	80	2	18	30	16	0	46
90	2	46	2	44	0	46	90	2	42	6	40	0	46	90	0	18	30	18	0	48
100	1	47	1	46	0	47	100	1	43	5	42	0	47	100	0	18	30	18	0	48
110	0	47	1	46	1	47	110	0	43	5	42	1	47	110	0	18	30	18	0	48
120	0	47	1	46	1	47	120	0	43	5	42	1	47	120	0	18	30	18	0	48
130	0	47	1	46	1	47	130	0	43	5	42	1	47	130	0	18	30	18	0	48
140	0	47	1	46	1	47	140	0	43	5	42	1	47	140	0	18	30	18	0	48
150	0	47	1	46	1	47	150	0	43	5	42	1	47	150	0	18	30	18	0	48
160	0	47	1	46	1	47	160	0	43	5	42	1	47	160	0	18	30	18	0	48
170	0	47	1	46	1	47	170	0	43	5	42	1	47	170	0	18	30	18	0	48
180	0	47	1	46	1	47	180	0	43	5	42	1	47	180	0	18	30	18	0	48

Tabla A.II.2.3. Datos de referencia *jamming* reactivo.

A.II.3 Tablas de datos de referencia para el tercer escenario de ataque, donde el nodo atacante está alejado del nodo coordinador de la red de sensores inalámbricos.

AODV							DSR							MPH						
t(s)	I(t)	C(t)	S(t)	R(t)	D(t)	A(t)	t(s)	I(t)	C(t)	S(t)	R(t)	D(t)	A(t)	t(s)	I(t)	C(t)	S(t)	R(t)	D(t)	A(t)
0	1	0	48	0	0	48	0	1	0	48	0	0	48	0	1	0	48	0	0	48
10	4	4	44	0	0	44	10	4	4	44	0	0	44	10	3	3	45	0	0	45
20	1	5	43	4	0	47	20	0	4	44	4	0	48	20	0	3	45	3	0	48
30	1	6	42	5	0	47	30	0	4	44	4	0	48	30	0	3	45	3	0	48
40	2	8	40	6	0	46	40	2	6	42	4	0	46	40	1	4	44	3	0	47
50	5	13	35	8	0	43	50	5	11	37	6	0	43	50	2	6	42	4	0	46
60	5	18	30	13	0	43	60	5	16	32	11	0	43	60	2	8	40	6	0	46
70	4	22	26	18	0	44	70	4	20	28	16	0	44	70	1	9	39	8	0	47
80	2	24	24	22	0	46	80	1	21	27	20	0	47	80	0	9	39	9	0	48
90	1	25	23	24	0	47	90	1	22	26	21	0	47	90	0	9	39	9	0	48
100	0	25	23	25	0	48	100	0	22	26	22	0	48	100	0	9	39	9	0	48
110	0	25	23	25	0	48	110	0	22	26	22	0	48	110	0	9	39	9	0	48
120	0	25	23	25	0	48	120	0	22	26	22	0	48	120	0	9	39	9	0	48
130	0	25	23	25	0	48	130	0	22	26	22	0	48	130	0	9	39	9	0	48
140	0	25	23	25	0	48	140	0	22	26	22	0	48	140	0	9	39	9	0	48
150	0	25	23	25	0	48	150	0	22	26	22	0	48	150	0	9	39	9	0	48
160	0	25	23	25	0	48	160	0	22	26	22	0	48	160	0	9	39	9	0	48
170	0	25	23	25	0	48	170	0	22	26	22	0	48	170	0	9	39	9	0	48
180	0	25	23	25	0	48	180	0	22	26	22	0	48	180	0	9	39	9	0	48

Tabla A.II.3.1. Datos de referencia *jamming* aleatorio 50 paquetes/segundo.

AODV							DSR							MPH						
t(s)	I(t)	C(t)	S(t)	R(t)	D(t)	A(t)	t(s)	I(t)	C(t)	S(t)	R(t)	D(t)	A(t)	t(s)	I(t)	C(t)	S(t)	R(t)	D(t)	A(t)
0	1	0	48	0	0	48	0	1	0	48	0	0	48	0	1	0	48	0	0	48
10	4	4	44	0	0	44	10	5	5	43	0	0	43	10	3	3	45	0	0	45
20	0	4	44	4	0	48	20	1	6	42	5	0	47	20	0	3	45	3	0	48
30	1	5	43	4	0	47	30	1	7	41	6	0	47	30	0	3	45	3	0	48
40	1	6	42	5	0	47	40	3	10	38	7	0	45	40	1	4	44	3	0	47
50	7	13	35	6	0	41	50	7	17	31	10	0	41	50	3	7	41	4	0	45
60	7	20	28	13	0	41	60	7	24	24	17	0	41	60	3	10	38	7	0	45
70	5	25	23	20	0	43	70	5	29	19	24	0	43	70	1	11	37	10	0	47
80	1	26	22	25	0	47	80	1	30	18	29	0	47	80	1	12	36	11	0	47
90	0	26	22	26	0	48	90	1	31	17	30	0	47	90	0	12	36	12	0	48
100	0	26	22	26	0	48	100	0	31	17	31	0	48	100	0	12	36	12	0	48
110	0	26	22	26	0	48	110	0	31	17	31	0	48	110	0	12	36	12	0	48
120	0	26	22	26	0	48	120	0	31	17	31	0	48	120	0	12	36	12	0	48
130	0	26	22	26	0	48	130	0	31	17	31	0	48	130	0	12	36	12	0	48
140	0	26	22	26	0	48	140	0	31	17	31	0	48	140	0	12	36	12	0	48
150	0	26	22	26	0	48	150	0	31	17	31	0	48	150	0	12	36	12	0	48
160	0	26	22	26	0	48	160	0	31	17	31	0	48	160	0	12	36	12	0	48
170	0	26	22	26	0	48	170	0	31	17	31	0	48	170	0	12	36	12	0	48
180	0	26	22	26	0	48	180	0	31	17	31	0	48	180	0	12	36	12	0	48

Tabla A.II.3.2. Datos de referencia *jamming* aleatorio 80 paquetes/segundo.

AODV							DSR						MPH							
t(s)	I(t)	C(t)	S(t)	R(t)	D(t)	A(t)	t(s)	I(t)	C(t)	S(t)	R(t)	D(t)	A(t)	t(s)	I(t)	C(t)	S(t)	R(t)	D(t)	A(t)
0	1	0	48	0	0	48	0	1	0	48	0	0	48	0	1	0	48	0	0	48
10	4	4	44	0	0	44	10	3	3	45	0	0	45	10	2	2	46	0	0	46
20	1	5	43	4	0	47	20	0	3	45	3	0	48	20	0	2	46	2	0	48
30	0	5	43	5	0	48	30	0	3	45	3	0	48	30	0	2	46	2	0	48
40	2	7	41	5	0	46	40	2	5	43	3	0	46	40	1	3	45	2	0	47
50	9	16	32	7	0	39	50	8	13	35	5	0	40	50	3	6	42	3	0	45
60	9	25	23	16	0	39	60	8	21	27	13	0	40	60	3	9	39	6	0	45
70	6	31	17	25	0	42	70	6	27	21	21	0	42	70	1	10	38	9	0	47
80	4	35	13	31	0	44	80	3	30	18	27	0	45	80	1	11	37	10	0	47
90	2	37	11	35	0	46	90	1	31	17	30	0	47	90	0	11	37	11	0	48
100	1	38	10	37	0	47	100	0	31	17	31	0	48	100	0	11	37	11	0	48
110	0	38	10	37	1	47	110	0	31	17	31	0	48	110	0	11	37	11	0	48
120	0	38	10	37	1	47	120	0	31	17	31	0	48	120	0	11	37	11	0	48
130	0	38	10	37	1	47	130	0	31	17	31	0	48	130	0	11	37	11	0	48
140	0	38	10	37	1	47	140	0	31	17	31	0	48	140	0	11	37	11	0	48
150	0	38	10	37	1	47	150	0	31	17	31	0	48	150	0	11	37	11	0	48
160	0	38	10	37	1	47	160	0	31	17	31	0	48	160	0	11	37	11	0	48
170	0	38	10	37	1	47	170	0	31	17	31	0	48	170	0	11	37	11	0	48
180	0	38	10	37	1	47	180	0	31	17	31	0	48	180	0	11	37	11	0	48

Tabla A.II.3.3. Datos de referencia *jamming* reactivo.

A.II.4.1 Tablas de datos experimentales obtenidos del estudio retrospectivo de propagación de ataques mediante el modelo epidémico SIR determinista. Primer escenario de ataque con nodo atacante próximo al nodo coordinador de red.

Protocolo	AODV			DSR			MPH		
	Estimado	95% I.C.		Estimado	95% I.C.		Estimado	95% I.C.	
Beta	0.0029	0.0026	0.0032	0.0030	0.0025	0.0036	0.0035	0.0024	0.0045
Gamma	0.0806	0.0686	0.0949	0.1068	0.0844	0.1289	0.1516	0.1017	0.2000
Nu	0.0008	0.0000	0.0020	0.0013	0.0000	0.0020	0.0011	0.0000	0.0020
Periodo ataque	12.4094	14.5867	10.5371	9.3604	11.8416	7.7572	6.5962	9.8349	5.0000
\mathcal{R}_0 teórico	1.7003	1.6070	1.8000	1.3424	1.2907	1.4132	1.0947	1.0543	1.1467
\mathcal{R}_0 modelo	1.7454	1.6549	1.8425	1.3932	1.3463	1.4541	1.1732	1.1446	1.2083

Tabla A.II.4.1. Parámetros caracterizadores del ataque *jamming* aleatorio a 50 paquetes/segundo contra cada uno de los protocolos para el primer escenario de ataque.

Protocolo	AODV		DSR		MPH	
	Modelo	Datos	Modelo	Datos	Modelo	Datos
\mathcal{R}_0 estimado	1.7454	1.6919	1.3932	1.3614	1.1732	1.1662
Pico nodos infectados	5.7042	7.0000	2.6763	5.0000	1.1750	4.0000
Pico ataque (s)	50.0000	50.0000	50.0000	50.0000	20.0000	10.0000
Nodos acumulados	34.0765	33.0000	24.1486	23.0000	13.4294	13.0000
Nodos susceptibles final ataque	13.9235	15.0000	23.8514	25.0000	34.5706	35.0000
Nodos caídos al final ataque	0.1956	0.0000	0.3806	0.0000	0.1334	0.0000

Tabla A.II.4.2. Comparativa de datos del ataque *jamming* aleatorio a 50 paquetes/segundo contra cada uno de los protocolos para el primer escenario de ataque.

Protocolo	AODV			DSR			MPH		
	Estimado	95% I.C.		Estimado	95% I.C.		Estimado	95% I.C.	
Beta	0.0029	0.0025	0.0033	0.0029	0.0026	0.0033	0.0033	0.0027	0.0040
Gamma	0.0894	0.0739	0.1041	0.0785	0.0670	0.0925	0.1265	0.0997	0.1584
Nu	0.0010	0.0000	0.0020	0.0008	0.0000	0.0020	0.0011	0.0000	0.0020
Periodo ataque	11.1905	13.5343	9.6045	12.7308	14.9279	10.8082	7.9037	10.0338	6.3136
\mathcal{R}_0 teórico	1.5415	1.4685	1.6299	1.7550	1.6564	1.8686	1.2530	1.2119	1.3036
\mathcal{R}_0 modelo	1.5874	1.5168	1.6707	1.8005	1.7038	1.9118	1.3105	1.2740	1.3545

Tabla A.II.4.3. Parámetros caracterizadores del ataque *jamming* aleatorio a 80 paquetes/segundo contra cada uno de los protocolos para el primer escenario de ataque.

Protocolo	AODV		DSR		MPH	
	Modelo	Datos	Modelo	Datos	Modelo	Datos
\mathcal{R}_0 estimado	1.5874	1.5340	1.8005	1.7395	1.3105	1.2936
Pico nodos infectados	4.2974	8.0000	6.2217	8.0000	2.0390	4.0000
Pico ataque (s)	50.0000	70.0000	50.0000	50.0000	40.0000	10.0000
Nodos acumulados	30.3082	29.0000	35.1423	34.0000	20.7701	20.0000
Nodos susceptibles final ataque	17.6918	19.0000	12.8577	14.0000	27.2299	28.0000
Nodos caídos al final ataque	0.3422	0.0000	0.1835	0.0000	0.2453	0.0000

Tabla A.II.4.4. Comparativa de datos del ataque *jamming* aleatorio a 80 paquetes/segundo contra cada uno de los protocolos para el primer escenario de ataque.

Protocolo	AODV			DSR			MPH		
	Estimado	95% I.C.		Estimado	95% I.C.		Estimado	95% I.C.	
Beta	0.0026	0.0023	0.0029	0.0025	0.0023	0.0028	0.0028	0.0021	0.0036
Gamma	0.0612	0.0531	0.0715	0.0678	0.0573	0.0785	0.1120	0.0793	0.1468
Nu	0.0008	0.0000	0.0020	0.0012	0.0000	0.0020	0.0011	0.0000	0.0020
Periodo ataque	16.3494	18.8468	13.9785	14.7539	17.4464	12.7382	8.9305	12.6087	6.8129
\mathcal{R}_0 teórico	1.9931	1.8526	2.1353	1.7697	1.6694	1.8887	1.1796	1.1262	1.2432
\mathcal{R}_0 modelo	2.0334	1.8968	2.1718	1.8088	1.7142	1.9220	1.2388	1.1978	1.2845

Tabla A.II.4.5. Parámetros caracterizadores del ataque *jamming* reactivo contra cada uno de los protocolos para el primer escenario de ataque.

Protocolo	AODV		DSR		MPH	
	Modelo	Datos	Modelo	Datos	Modelo	Datos
\mathcal{R}_0 estimado	2.0334	1.9814	1.8088	1.7395	1.1978	1.2164
Pico nodos infectados	8.2726	9.0000	6.3484	8.0000	1.5700	4.0000
Pico ataque (s)	60.0000	50.0000	60.0000	50.0000	40.0000	50.0000
Nodos acumulados	38.6868	38.0000	35.2682	34.0000	17.2305	16.0000
Nodos susceptibles final ataque	9.3132	10.0000	12.7318	14.0000	30.7695	32.0000
Nodos caídos al final ataque	0.3634	1.0000	0.7882	1.0000	0.2258	0.0000

Tabla A.II.4.6. Comparativa de datos del ataque *jamming* reactivo contra cada uno de los protocolos para el primer escenario de ataque.

A.II.4.2 Tablas de datos experimentales obtenidos del estudio retrospectivo de propagación de ataques mediante el modelo epidémico SIR determinista. Segundo escenario de ataque con nodo atacante centrado en la topología de red.

Protocolo	AODV			DSR			MPH		
	Estimado	95% I.C.		Estimado	95% I.C.		Estimado	95% I.C.	
Beta	0.0028	0.0025	0.0031	0.0029	0.0026	0.0033	0.0035	0.0026	0.0046
Gamma	0.0679	0.0583	0.0792	0.0813	0.0687	0.0957	0.1447	0.1056	0.2000
Nu	0.0012	0.0000	0.0020	0.0008	0.0000	0.0020	0.0011	0.0000	0.0020
Periodo ataque	14.7363	17.1544	12.6309	12.2946	14.5532	10.4507	6.9107	9.4677	5.0000
\mathcal{R}_0 teórico	1.9266	1.8049	2.0689	1.7089	1.6172	1.8125	1.1412	1.1011	1.1888
\mathcal{R}_0 modelo	1.9711	1.8500	2.1091	1.7546	1.6640	1.8553	1.2111	1.1797	1.2477

Tabla A.II.4.7. Parámetros caracterizadores del ataque *jamming* aleatorio a 50 paquetes/segundo contra cada uno de los protocolos para el segundo escenario de ataque.

Protocolo	AODV		DSR		MPH	
	Modelo	Datos	Modelo	Datos	Modelo	Datos
\mathcal{R}_0 estimado	1.9711	1.9113	1.7546	1.6919	1.2111	1.1990
Pico nodos infectados	7.6337	8.0000	5.8112	8.0000	1.3709	4.0000
Pico ataque (s)	50.0000	50.0000	50.0000	50.0000	30.0000	10.0000
Nodos acumulados	37.8696	37.0000	34.2569	33.0000	15.6370	15.0000
Nodos susceptibles final ataque	10.1304	11.0000	13.7431	15.0000	32.3630	33.0000
Nodos caídos al final ataque	0.8238	1.0000	0.2152	0.0000	0.1629	0.0000

Tabla A.II.4.8. Comparativa de datos del ataque *jamming* aleatorio a 50 paquetes/segundo contra cada uno de los protocolos para el segundo escenario de ataque.

Protocolo	AODV			DSR			MPH		
	Estimado	95% I.C.		Estimado	95% I.C.		Estimado	95% I.C.	
Beta	0.0028	0.0025	0.0031	0.0028	0.0026	0.0030	0.0031	0.0026	0.0038
Gamma	0.0654	0.0566	0.0760	0.0569	0.0494	0.0660	0.1186	0.0949	0.1465
Nu	0.0005	0.0000	0.0020	0.0005	0.0000	0.0020	0.0012	0.0000	0.0020
Periodo ataque	15.2894	17.6821	13.1608	17.5784	20.2289	15.1509	8.4294	10.5372	6.8241
\mathcal{R}_0 teórico	2.0168	1.8697	2.1786	2.3426	2.1354	2.5598	1.2597	1.2147	1.3092
\mathcal{R}_0 modelo	2.0617	1.9167	2.2222	2.3898	2.1842	2.6072	1.3156	1.2761	1.3593

Tabla A.II.4.9. Parámetros caracterizadores del ataque *jamming* aleatorio a 80 paquetes/segundo contra cada uno de los protocolos para el segundo escenario de ataque.

Protocolo	AODV		DSR		MPH	
	Modelo	Datos	Modelo	Datos	Modelo	Datos
\mathcal{R}_0 estimado	2.0617	1.9814	2.3898	2.3765	1.3156	1.2936
Pico nodos infectados	8.3722	9.0000	11.0094	10.0000	2.0746	4.0000
Pico ataque (s)	50.0000	50.0000	50.0000	50.0000	50.0000	50.0000
Nodos acumulados	38.9858	38.0000	42.0948	42.0000	21.0229	20.0000
Nodos susceptibles final ataque	9.0142	10.0000	5.9052	6.0000	26.9771	28.0000
Nodos caídos al final ataque	0.0349	0.0000	0.0633	0.0000	0.2776	0.0000

Tabla A.II.4.10. Comparativa de datos del ataque *jamming* aleatorio a 80 paquetes/segundo contra cada uno de los protocolos para el segundo escenario de ataque.

Protocolo	AODV			DSR			MPH		
	Estimado	95% I.C.		Estimado	95% I.C.		Estimado	95% I.C.	
Beta	0.0027	0.0025	0.0028	0.0026	0.0024	0.0028	0.0030	0.0023	0.0037
Gamma	0.0453	0.0388	0.0520	0.0514	0.0440	0.0599	0.1176	0.0856	0.1488
Nu	0.0004	0.0000	0.0019	0.0004	0.0000	0.0020	0.0012	0.0000	0.0020
Periodo ataque	22.0816	25.7613	19.2172	19.4405	22.7027	16.6853	8.5055	11.6760	6.7213
\mathcal{R}_0 teórico	2.8006	2.5359	3.1214	2.4095	2.1915	2.6505	1.2176	1.1714	1.2760
\mathcal{R}_0 modelo	2.8435	2.5833	3.1580	2.4511	2.2378	2.6900	1.2756	1.2365	1.3197

Tabla A.II.4.11. Parámetros caracterizadores del ataque *jamming* reactivo contra cada uno de los protocolos para el segundo escenario de ataque.

Protocolo	AODV		DSR		MPH	
	Modelo	Datos	Modelo	Datos	Modelo	Datos
\mathcal{R}_0 estimado	2.8435	3.9536	2.4511	2.5248	1.2756	1.2533
Pico nodos infectados	13.9133	10.0000	11.2945	10.0000	1.7958	4.0000
Pico ataque (s)	50.0000	50.0000	60.0000	50.0000	40.0000	50.0000
Nodos acumulados	44.4935	47.0000	42.4991	43.0000	19.1068	18.0000
Nodos susceptibles final ataque	3.5065	1.0000	5.5009	5.0000	28.8932	30.0000
Nodos caídos al final ataque	0.0000	1.0000	0.0000	1.0000	0.2658	0.0000

Tabla A.II.4.12. Comparativa de datos del ataque *jamming* reactivo contra cada uno de los protocolos para el segundo escenario de ataque.

A.II.4.3 Tablas de datos experimentales obtenidos del estudio retrospectivo de propagación de ataques mediante el modelo epidémico SIR determinista. Tercer escenario de ataque con nodo atacante alejado del nodo coordinador de red.

Protocolo	AODV			DSR			MPH		
	Estimado	95% I.C.		Estimado	95% I.C.		Estimado	95% I.C.	
Beta	0.0031	0.0026	0.0036	0.0031	0.0026	0.0037	0.0031	0.0018	0.0042
Gamma	0.1070	0.0868	0.1268	0.1120	0.0911	0.1384	0.1478	0.0820	0.2000
Nu	0.0013	0.0000	0.0020	0.0012	0.0000	0.0020	0.0011	0.0000	0.0020
Periodo ataque	9.3485	11.5229	7.8873	8.9303	10.9777	7.2257	6.7674	12.2008	5.0000
\mathcal{R}_0 teórico	1.3910	1.3389	1.4582	1.3106	1.2598	1.3665	1.0087	0.9605	1.0662
\mathcal{R}_0 modelo	1.4412	1.3926	1.5072	1.3633	1.3174	1.4105	1.1126	1.0866	1.1439

Tabla A.II.4.13. Parámetros caracterizadores del ataque *jamming* aleatorio a 50 paquetes/segundo contra cada uno de los protocolos para el tercer escenario de ataque.

Protocolo	AODV		DSR		MPH	
	Modelo	Datos	Modelo	Datos	Modelo	Datos
\mathcal{R}_0 estimado	1.4412	1.4126	1.3633	1.3377	1.1126	1.1074
Pico nodos infectados	3.0502	5.0000	2.4386	5.0000	1.0000	3.0000
Pico ataque (s)	50.0000	50.0000	50.0000	50.0000	0.0000	10.0000
Nodos acumulados	25.9062	25.0000	23.0138	22.0000	9.2701	9.0000
Nodos susceptibles final ataque	22.0938	23.0000	24.9862	26.0000	38.7299	39.0000
Nodos caídos al final ataque	0.4170	0.0000	0.3261	0.0000	0.0946	0.0000

Tabla A.II.4.14. Comparativa de datos del ataque *jamming* aleatorio a 50 paquetes/segundo contra cada uno de los protocolos para el tercer escenario de ataque.

Protocolo	AODV			DSR			MPH		
	Estimado	95% I.C.		Estimado	95% I.C.		Estimado	95% I.C.	
Beta	0.0031	0.0026	0.0036	0.0031	0.0027	0.0036	0.0030	0.0021	0.0044
Gamma	0.1022	0.0831	0.1255	0.0915	0.0768	0.1082	0.1347	0.0891	0.2000
Nu	0.0013	0.0000	0.0020	0.0011	0.0000	0.0020	0.0011	0.0000	0.0020
Periodo ataque	9.7812	12.0408	7.9660	10.9251	13.0223	9.2423	7.4230	11.2252	5.0000
\mathcal{R}_0 teórico	1.4303	1.3730	1.4985	1.6050	1.5225	1.6803	1.0811	1.0351	1.1365
\mathcal{R}_0 modelo	1.4792	1.4260	1.5440	1.6521	1.5713	1.7265	1.1608	1.1311	1.1952

Tabla A.II.4.15. Parámetros caracterizadores del ataque *jamming* aleatorio a 80 paquetes/segundo contra cada uno de los protocolos para el tercer escenario de ataque.

Protocolo	AODV		DSR		MPH	
	Modelo	Datos	Modelo	Datos	Modelo	Datos
\mathcal{R}_0 estimado	1.4792	1.4403	1.6521	1.6072	1.1608	1.1507
Pico nodos infectados	3.3791	7.0000	4.9185	7.0000	1.1291	3.0000
Pico ataque (s)	50.0000	50.0000	50.0000	50.0000	20.0000	10.0000
Nodos acumulados	27.2339	26.0000	32.0806	31.0000	12.6262	12.0000
Nodos susceptibles final ataque	20.7661	22.0000	15.9194	17.0000	35.3738	36.0000
Nodos caídos al final ataque	0.4537	0.0000	0.4713	0.0000	0.1393	0.0000

Tabla A.II.4.16. Comparativa de datos del ataque *jamming* aleatorio a 80 paquetes/segundo contra cada uno de los protocolos para el tercer escenario de ataque.

Protocolo	AODV			DSR			MPH		
	Estimado	95% I.C.		Estimado	95% I.C.		Estimado	95% I.C.	
Beta	0.0026	0.0023	0.0028	0.0027	0.0023	0.0031	0.0028	0.0019	0.0042
Gamma	0.0610	0.0520	0.0697	0.0785	0.0653	0.0935	0.1251	0.0788	0.1985
Nu	0.0009	0.0000	0.0020	0.0009	0.0000	0.0020	0.0011	0.0000	0.0020
Periodo ataque	16.3889	19.2460	14.3388	12.7376	15.3065	10.6960	7.9959	12.6932	5.0381
\mathcal{R}_0 teórico	1.9934	1.8750	2.1665	1.6318	1.5470	1.7306	1.0638	1.0112	1.1267
\mathcal{R}_0 modelo	2.0337	1.9177	2.2002	1.6743	1.5935	1.7699	1.1462	1.1151	1.1797

Tabla A.II.4.17. Parámetros caracterizadores del ataque *jamming* reactivo contra cada uno de los protocolos para el tercer escenario de ataque.

Protocolo	AODV		DSR		MPH	
	Modelo	Datos	Modelo	Datos	Modelo	Datos
\mathcal{R}_0 estimado	2.0337	1.9814	1.6743	1.6072	1.1462	1.1358
Pico nodos infectados	8.1714	9.0000	5.1401	8.0000	1.0800	3.0000
Pico ataque (s)	60.0000	50.0000	60.0000	50.0000	20.0000	50.0000
Nodos acumulados	38.6087	38.0000	32.6576	31.0000	11.6601	11.0000
Nodos susceptibles final ataque	9.3913	10.0000	15.3424	17.0000	36.3399	37.0000
Nodos caídos al final ataque	0.5102	1.0000	0.3060	0.0000	0.1382	0.0000

Tabla A.II.4.18. Comparativa de datos del ataque *jamming* reactivo contra cada uno de los protocolos para el tercer escenario de ataque.

A.II.4.4 Tablas de datos experimentales obtenidos del estudio predictivo de propagación de ataques mediante el modelo de Crecimiento Logístico Generalizado GLGM. Primer escenario de ataque con nodo atacante próximo al nodo coordinador de red.

Protocolo	AODV			DSR			MPH		
Parámetro	Estimado	95% I.C.		Estimado	95% I.C.		Estimado	95% I.C.	
r	0.0564	0.0394	0.0953	0.0533	0.0338	0.1096	0.1522	0.0353	0.2354
p	1.1491	0.7253	1.2000	1.1164	0.4067	1.2000	0.6953	0.0100	1.2000
K	34.7217	12.6518	43.2000	33.5514	8.2273	43.2000	16.7362	5.0399	43.2000
\mathcal{R}_0 modelo	1.7765	1.1608	2.5584	1.7176	1.0970	2.5584	1.2296	1.0565	2.5584
\mathcal{R}_0 datos	1.6919			1.3614			1.1662		
K datos	33			23			13		

Tabla A.II.4.19. Parámetros caracterizadores del ataque *jamming* aleatorio a 50 paquetes/segundo contra cada uno de los protocolos para el primer escenario de ataque.

Protocolo	AODV			DSR			MPH		
Parámetro	Estimado	95% I.C.		Estimado	95% I.C.		Estimado	95% I.C.	
r	0.0550	0.0392	0.1198	0.0570	0.0428	0.1075	0.1850	0.0531	0.3019
p	1.1471	0.6576	1.2000	1.1565	0.7604	1.2000	0.5415	0.0100	0.9494
K	35.2808	12.7138	43.2000	35.5938	13.7597	43.2000	22.6603	7.2891	43.2000
\mathcal{R}_0 modelo	1.8069	1.1617	2.5584	1.8246	1.1784	2.5584	1.3532	1.0846	2.5584
\mathcal{R}_0 datos	1.5340			1.7395			1.2936		
K datos	29			34			20		

Tabla A.II.4.20. Parámetros caracterizadores del ataque *jamming* aleatorio a 80 paquetes/segundo contra cada uno de los protocolos para el primer escenario de ataque.

Protocolo	AODV			DSR			MPH		
Parámetro	Estimado	95% I.C.		Estimado	95% I.C.		Estimado	95% I.C.	
r	0.0566	0.0425	0.0969	0.0540	0.0406	0.0875	0.0507	0.0292	0.1121
p	1.1684	0.8636	1.2000	1.1633	0.7951	1.2000	1.1177	0.2902	1.2000
K	36.2517	17.2982	43.2000	36.7818	13.3061	43.2000	31.6190	7.2279	43.2000
\mathcal{R}_0 modelo	1.8636	1.2400	2.5584	1.8970	1.1711	2.5584	1.6321	1.0838	2.5584
\mathcal{R}_0 datos	1.9814			1.7395			1.2164		
K datos	38			34			16		

Tabla A.II.4.21. Parámetros caracterizadores del ataque *jamming* reactivo contra cada uno de los protocolos para el primer escenario de ataque.

A.II.4.5 Tablas de datos experimentales obtenidos del estudio predictivo de propagación de ataques mediante el modelo de Crecimiento Logístico Generalizado GLGM. Segundo escenario de ataque con nodo atacante centrado en la topología de red.

Protocolo	AODV			DSR			MPH		
Parámetro	Estimado	95% I.C.		Estimado	95% I.C.		Estimado	95% I.C.	
r	0.0568	0.0433	0.0930	0.0568	0.0424	0.0882	0.1432	0.0368	0.2745
p	1.1616	0.8094	1.2000	1.1611	0.8594	1.2000	0.7464	0.0100	1.2000
K	37.2822	17.5267	43.2000	37.2953	16.7808	43.2000	20.1826	6.1579	43.2000
\mathcal{R}_0 modelo	1.9303	1.2443	2.5584	1.9312	1.2305	2.5584	1.2974	1.0702	2.5584
\mathcal{R}_0 datos	1.9113			1.6919			1.1990		
K datos	37			33			15		

Tabla A.II.4.22. Parámetros caracterizadores del ataque *jamming* aleatorio a 50 paquetes/segundo contra cada uno de los protocolos para el segundo escenario de ataque.

Protocolo	AODV			DSR			MPH		
Parámetro	Estimado	95% I.C.		Estimado	95% I.C.		Estimado	95% I.C.	
r	0.0589	0.0453	0.0974	0.0609	0.0467	0.0953	0.0517	0.0315	0.1012
p	1.1639	0.8613	1.2000	1.1620	0.8539	1.2000	1.1321	0.5428	1.2000
K	37.9750	18.5029	43.2000	37.9144	22.0856	43.2000	31.4617	7.1999	43.2000
\mathcal{R}_0 modelo	1.9796	1.2631	2.5584	1.9751	1.3397	2.5584	1.6256	1.0835	2.5584
\mathcal{R}_0 datos	1.9814			2.3765			1.2936		
K datos	38			42			20		

Tabla A.II.4.23. Parámetros caracterizadores del ataque *jamming* aleatorio a 80 paquetes/segundo contra cada uno de los protocolos para el segundo escenario de ataque.

Protocolo	AODV			DSR			MPH		
Parámetro	Estimado	95% I.C.		Estimado	95% I.C.		Estimado	95% I.C.	
r	0.0616	0.0481	0.0947	0.0602	0.0470	0.0836	0.0523	0.0338	0.1104
p	0.0616	0.0481	0.0947	1.1761	0.9654	1.2000	1.1425	0.4942	1.2000
K	38.7963	22.2507	43.2000	39.6930	22.8748	43.2000	31.4010	8.5674	43.2000
\mathcal{R}_0 modelo	2.0434	1.3435	2.5584	2.1212	1.3583	2.5584	1.6232	1.1015	2.5584
\mathcal{R}_0 datos	3.9536			2.5248			1.2533		
K datos	47			43			18		

Tabla A.II.4.24. Parámetros caracterizadores del ataque *jamming* reactivo contra cada uno de los protocolos para el segundo escenario de ataque.

A.II.4.6 Tablas de datos experimentales obtenidos del estudio predictivo de propagación de ataques mediante el modelo de Crecimiento Logístico Generalizado GLGM. Tercer escenario de ataque con nodo atacante alejado del nodo coordinador de red.

Protocolo	AODV			DSR			MPH		
Parámetro	Estimado	95% I.C.		Estimado	95% I.C.		Estimado	95% I.C.	
r	0.0526	0.0343	0.0992	0.0524	0.0343	0.1133	0.1371	0.0315	0.2143
p	1.1338	0.5286	1.2000	1.1374	0.5626	1.2000	0.7923	0.0100	1.2000
K	33.7343	8.6718	43.2000	34.4252	10.3454	43.2000	12.3636	3.3271	43.2000
\mathcal{R}_0 modelo	1.7264	1.1029	2.5584	1.7610	1.1263	2.5584	1.1563	1.0363	2.5584
\mathcal{R}_0 datos	1.4126			1.3377			1.1074		
K datos	25			22			9		

Tabla A.II.4.25. Parámetros caracterizadores del ataque *jamming* aleatorio a 50 paquetes/segundo contra cada uno de los protocolos para el tercer escenario de ataque.

Protocolo	AODV			DSR			MPH		
Parámetro	Estimado	95% I.C.		Estimado	95% I.C.		Estimado	95% I.C.	
r	0.0531	0.0381	0.0995	0.0546	0.0394	0.0952	0.0507	0.0257	0.1285
p	1.1633	0.7810	1.2000	1.1622	0.7691	1.2000	1.0903	0.2590	1.2000
K	35.0555	12.3244	43.2000	36.5691	13.9279	43.2000	30.2446	4.8856	43.2000
\mathcal{R}_0 modelo	1.7945	1.1557	2.5584	1.8834	1.1811	2.5584	1.5784	1.0546	2.5584
\mathcal{R}_0 datos	1.4403			1.6072			1.1507		
K datos	26			31			12		

Tabla A.II.4.26. Parámetros caracterizadores del ataque *jamming* aleatorio a 80 paquetes/segundo contra cada uno de los protocolos para el tercer escenario de ataque.

Protocolo	AODV			DSR			MPH		
Parámetro	Estimado	95% I.C.		Estimado	95% I.C.		Estimado	95% I.C.	
r	0.0561	0.0403	0.0903	0.0546	0.0392	0.0893	0.0539	0.0250	0.1376
p	1.1598	0.7408	1.2000	1.1569	0.7636	1.2000	1.0756	0.0608	1.2000
K	37.8822	17.0327	43.2000	37.1989	15.8195	43.2000	30.1963	4.3477	43.2000
\mathcal{R}_0 modelo	1.9727	1.2351	2.5584	1.9246	1.2132	2.5584	1.5766	1.0482	2.5584
\mathcal{R}_0 datos	1.9814			1.6072			1.1358		
K datos	38			31			11		

Tabla A.II.4.27. Parámetros caracterizadores del ataque *jamming* reactivo contra cada uno de los protocolos para el tercer escenario de ataque.

APÉNDICE

III

Relación de figuras representativas obtenidas de los diferentes experimentos

En el desarrollo de esta investigación, el conjunto de experimentos realizados ha generado un total de aproximadamente 432 figuras, correspondientes a un total de 108 casos de estudio para los diferentes modelos epidemiológicos y escenarios de ataque. Sin embargo, en aras de no extender la memoria de Tesis, en este Apéndice se presentan una serie de figuras representativas donde pueden observarse los resultados más relevantes obtenidos en los diferentes experimentos. Estos resultados experimentales son suficientemente representativos como para determinar la validez de cada uno de los modelos epidemiológicos propuestos, así como para demostrar la validez de la hipótesis planteada en esta Tesis. En cada uno de los siguientes apartados, se indica para cada modelo propuesto, el caso de estudio concreto que se utiliza como ejemplo de las figuras obtenidas.

Finalmente, comentar que el código MATLAB generado para la realización de los experimentos y simulaciones presentados en esta Memoria de Tesis, así como los archivos con los datos de referencia utilizados para la realización de los experimentos pueden encontrarse en el siguiente repositorio:

https://github.com/BioSIP/jamming_epidemiology.git

A.III.1.1 Estudio retrospectivo de propagación de ataques mediante el modelo epidémico SIR determinista. Caso de *jamming* reactivo contra AODV. Primer escenario de ataque con nodo atacante próximo al nodo coordinador de red.

Figura A.III.1.1.

Las gráficas (a), (b), (c) y (d) muestran el mejor ajuste inicial del modelo para cada una de las curvas $dS(t)/dt$, $dI(t)/dt$, $dR(t)/dt$ y $dD(t)/dt$. La línea roja continua representa la curva característica del ataque para cada uno de los grupos de nodos, según el modelo SIRD propuesto para este experimento. Los círculos azules representan los datos de referencia. En misma figura, las gráficas (e), (f), (g) y (h) muestra los residuos en función del tiempo.

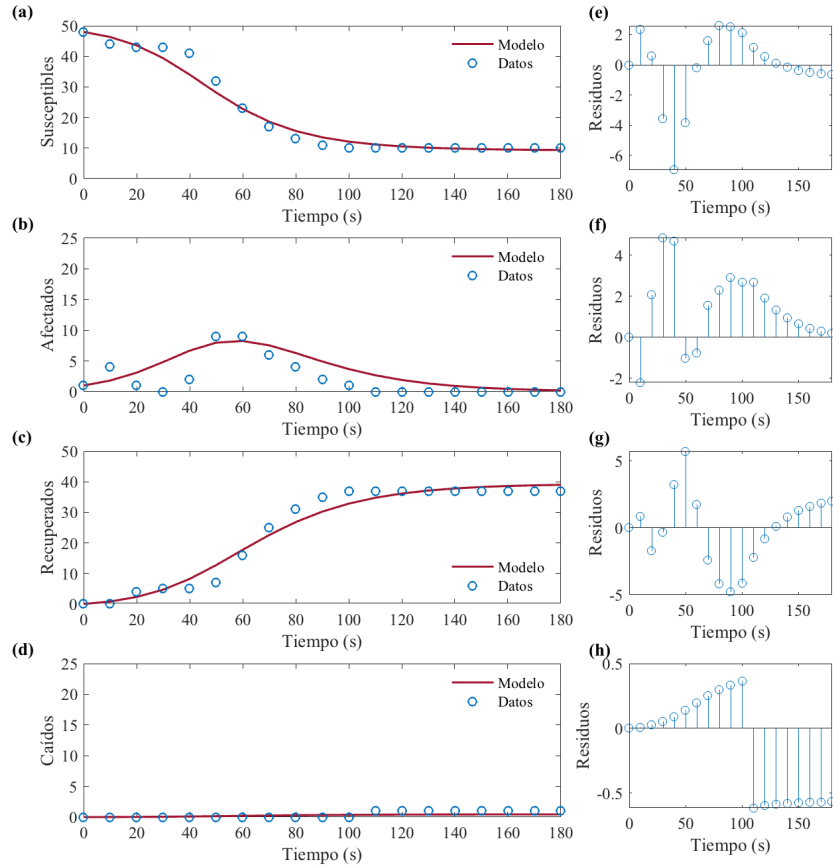


Figura A.III.1.2.

Histogramas con los valores del 95% del intervalo de confianza obtenido para los parámetros β , γ , y ν , gráficas (a), (b) y (c), respectivamente. El histograma (d) representa el intervalo de confianza estimado al 95% del número reproductivo básico \mathcal{R}_0 .

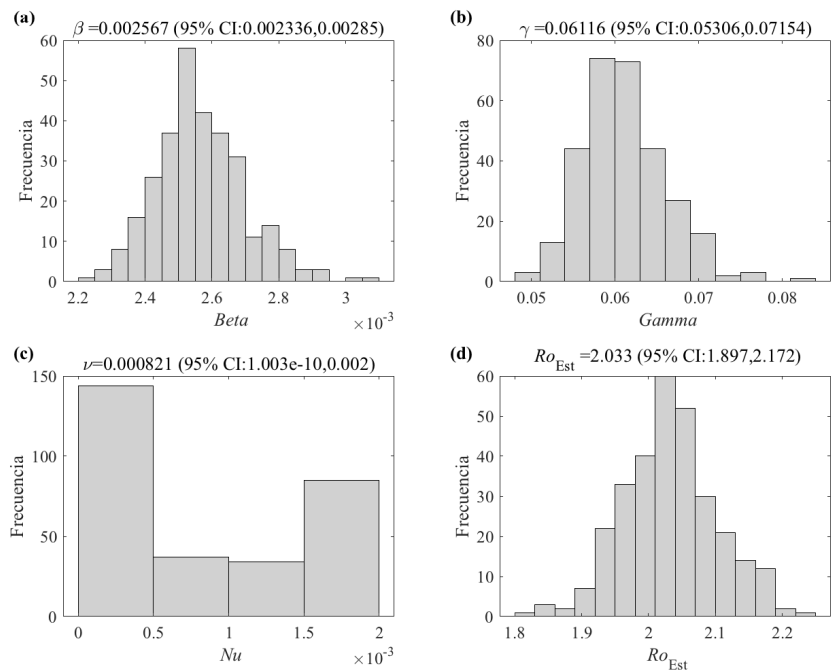


Figura A.III.1.3.

Las gráficas (a), (b), (c) y (d) muestran el mejor ajuste del modelo para cada una de las curvas $dS(t)/dt$, $dI(t)/dt$, $dR(t)/dt$ y $dD(t)/dt$. La línea roja continua representa la curva característica del ataque para cada uno de los grupos de nodos, según el modelo SIRD propuesto para este experimento. Los círculos azules representan los datos de referencia. Los trazos de línea gris claro representan cada una de las 300 realizaciones de obtenidas con la estructura de error de la distribución de *Poisson*.

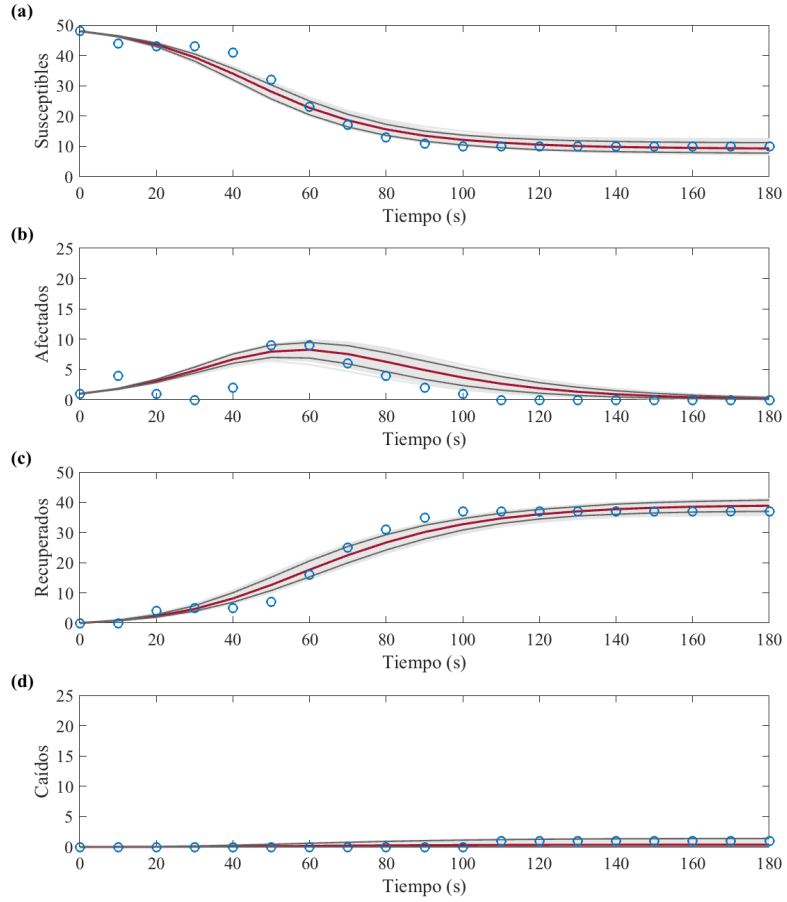


Figura A.III.1.4.

Incidencia acumulada según modelo, línea roja, intervalo de confianza al 95%, líneas grises, e incidencia acumulada según datos de referencia, línea azul.

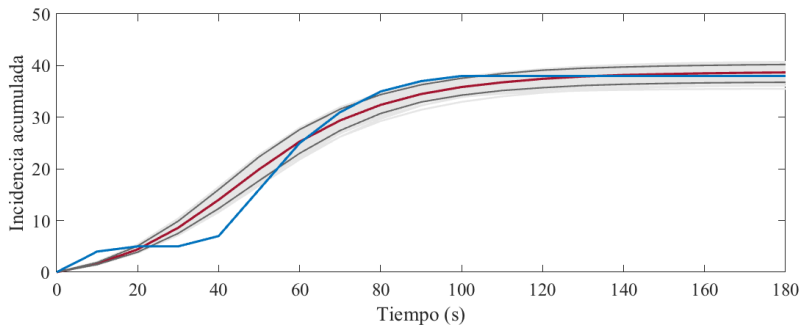
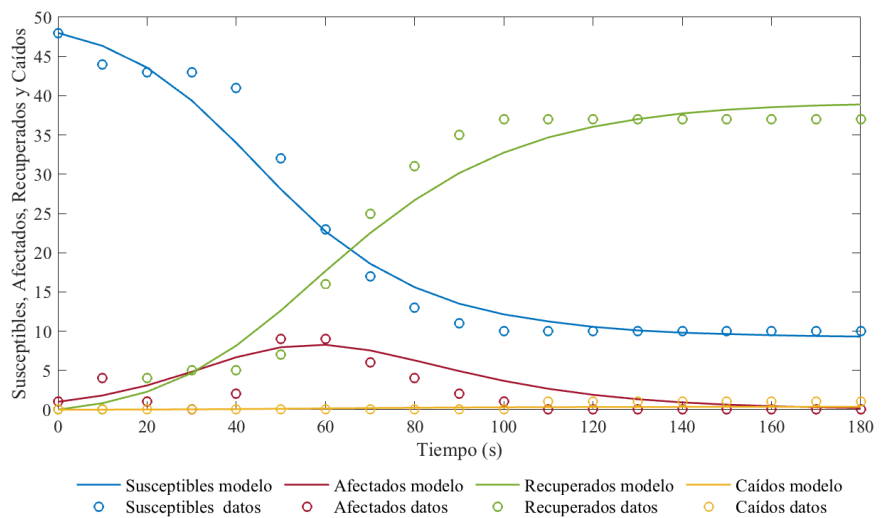


Figura A.III.1.5.

Comparativa de los resultados experimentales obtenidos por el modelo propuesto, trazos de línea continua coloreada, con respecto a los datos de referencia, círculos coloreados.



A.III.1.2 Estudio retrospectivo de propagación de ataques mediante el modelo epidémico SIR determinista. Caso de *jamming* aleatorio a 80 p/s contra DSR. Segundo escenario de ataque con nodo atacante centrado en la topología de red.

Figura A.III.1.6.

Las gráficas (a), (b), (c) y (d) muestran el mejor ajuste inicial del modelo para cada una de las curvas $dS(t)/dt$, $dI(t)/dt$, $dR(t)/dt$ y $dD(t)/dt$. La línea roja continua representa la curva característica del ataque para cada uno de los grupos de nodos, según el modelo SIRD propuesto para este experimento. Los círculos azules representan los datos de referencia. En misma figura, las gráficas (e), (f), (g) y (h) muestra los residuos en función del tiempo.

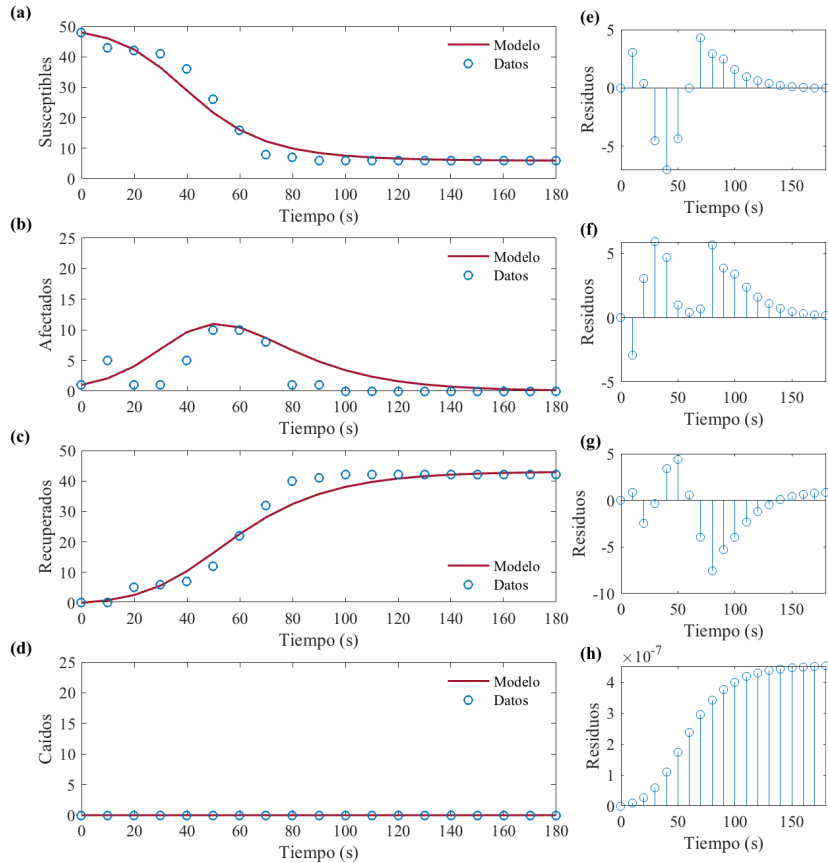


Figura A.III.1.7.

Histogramas con los valores del 95% del intervalo de confianza obtenido para los parámetros β , γ , y ν , gráficas (a), (b) y (c), respectivamente. El histograma (d) representa el intervalo de confianza estimado al 95% del número reproductivo básico \mathcal{R}_0 .

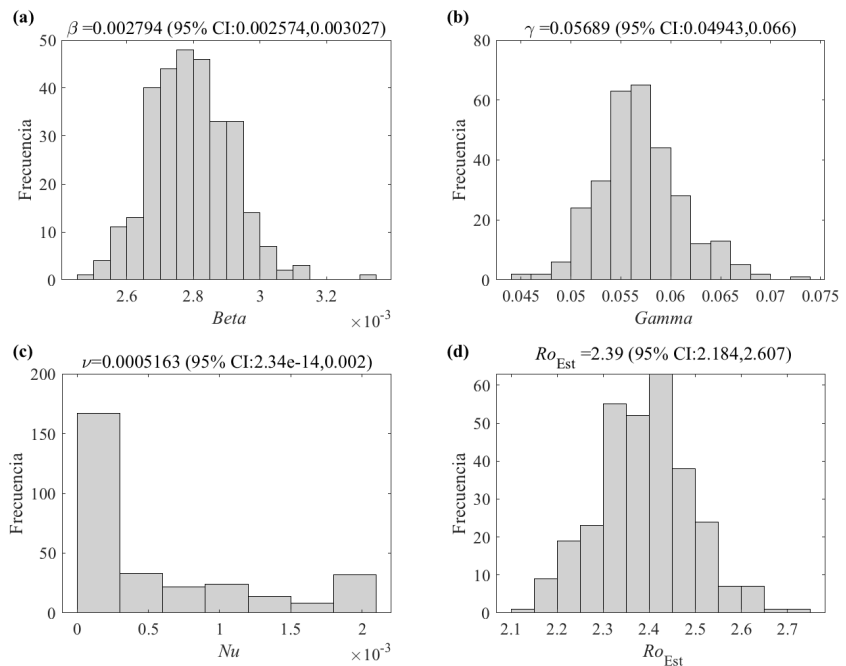


Figura A.III.1.8.

Las gráficas (a), (b), (c) y (d) muestran el mejor ajuste del modelo para cada una de las curvas $dS(t)/dt$, $dI(t)/dt$, $dR(t)/dt$ y $dD(t)/dt$. La línea roja continua representa la curva característica del ataque para cada uno de los grupos de nodos, según el modelo SIRD propuesto para este experimento. Los círculos azules representan los datos de referencia. Los trazos de línea gris claro representan cada una de las 300 realizaciones de obtenidas con la estructura de error de la distribución de *Poisson*.

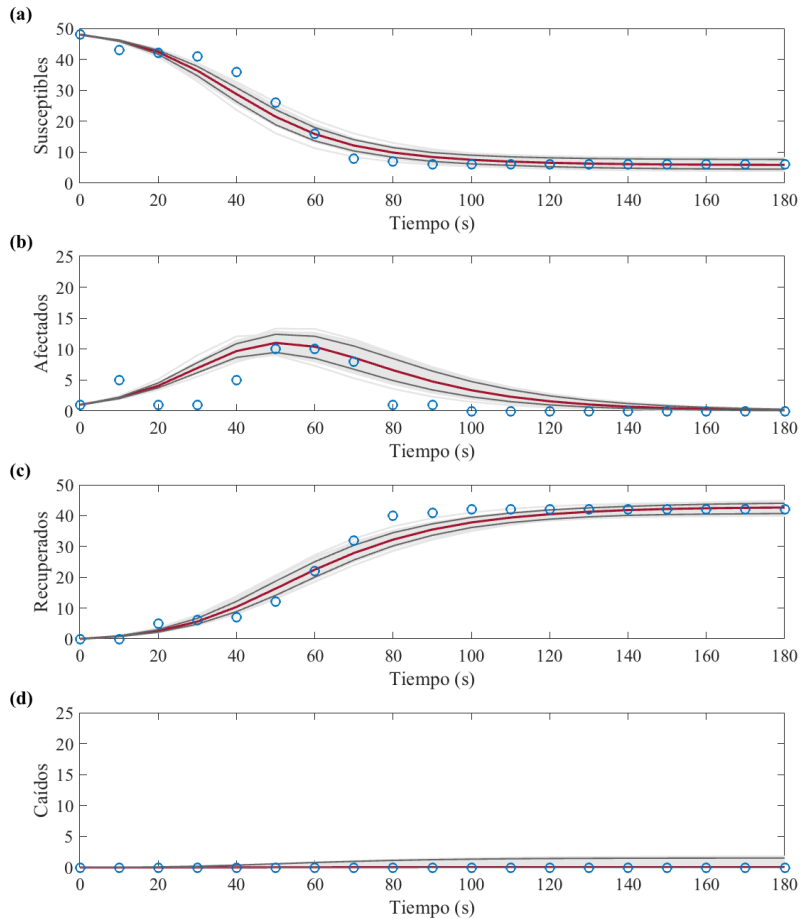


Figura A.III.1.9.

Incidencia acumulada según modelo, línea roja, intervalo de confianza al 95%, líneas grises, e incidencia acumulada según datos de referencia, línea azul.

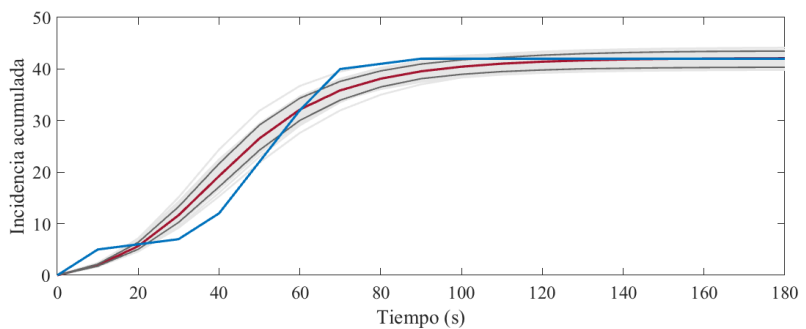
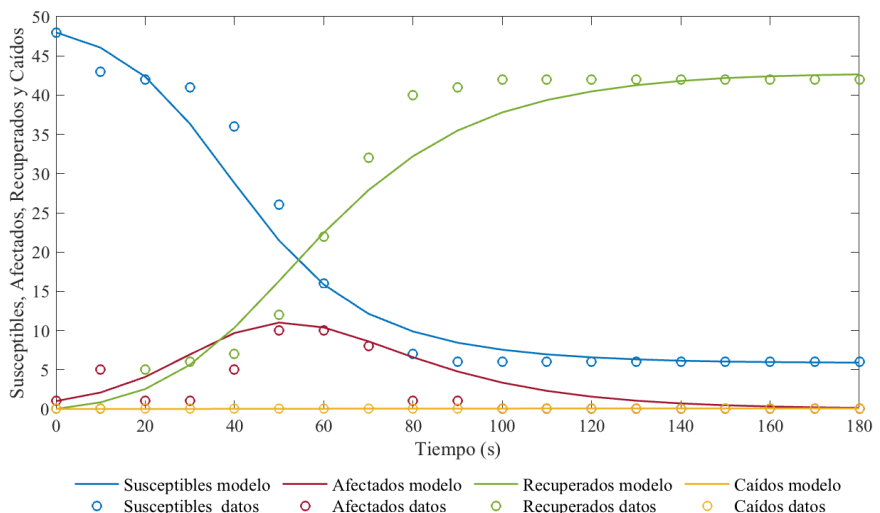


Figura A.III.1.10.

Comparativa de los resultados experimentales obtenidos por el modelo propuesto, trazos de línea continua coloreada, con respecto a los datos de referencia, círculos coloreados.



A.III.2.1 Estudio predictivo de propagación de ataques mediante el modelo epidémico SIR determinista. Caso de *jamming* reactivo contra DSR. Segundo escenario de ataque con nodo atacante centrado en la topología de red.

Figura A.III.2.1.

Las gráficas (a), (b), (c) y (d) muestran el mejor ajuste inicial del modelo en la etapa temprana del ataque, para cada una de las curvas $dS(t)/dt$, $dI(t)/dt$, $dR(t)/dt$ y $dD(t)/dt$. La línea roja continua representa la curva característica del ataque para cada uno de los grupos de nodos, según el modelo SIRD propuesto para este experimento. Los círculos azules representan los datos de referencia. En misma figura, las gráficas (e), (f), (g) y (h) muestra los residuos en función del tiempo.

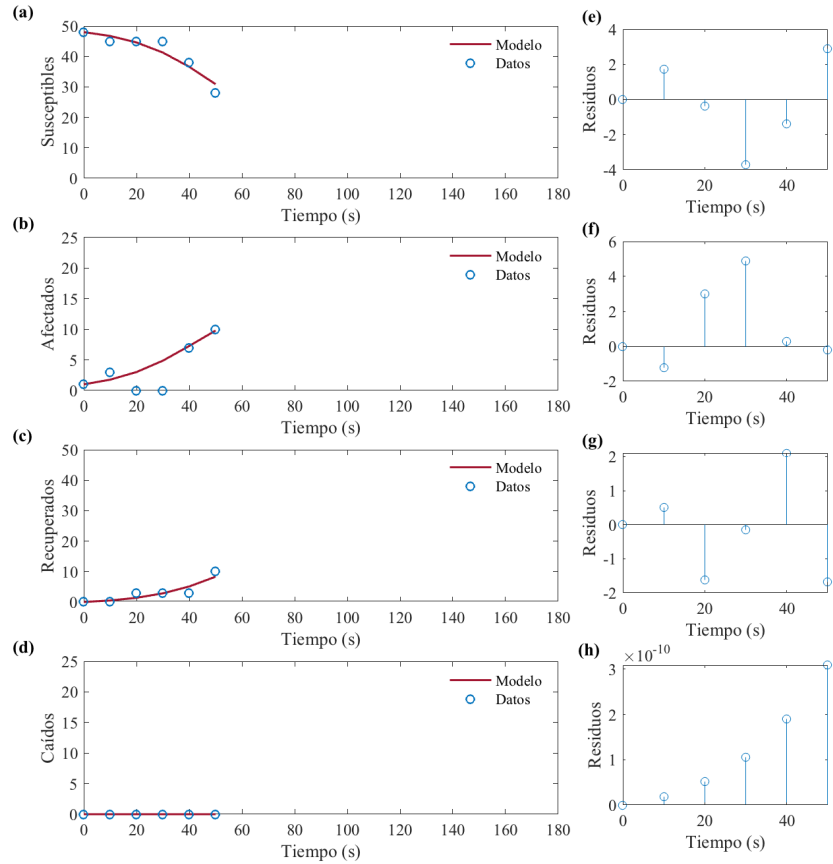


Figura A.III.2.2.

Histogramas con los valores del 95% del intervalo de confianza obtenido para los parámetros β , γ , y ν , gráficas (a), (b) y (c), respectivamente. El histograma (d) representa el intervalo de confianza estimado al 95% del número reproductivo básico \mathcal{R}_0 .

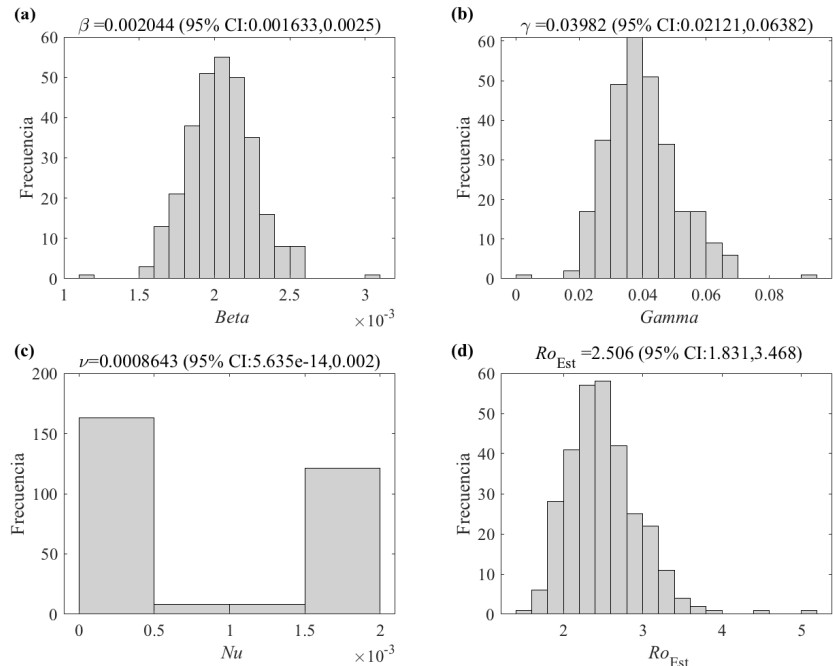


Figura A.III.2.3.

Las gráficas (a), (b), (c) y (d) muestran el mejor ajuste del modelo para cada una de las curvas $dS(t)/dt$, $dI(t)/dt$, $dR(t)/dt$ y $dD(t)/dt$. La línea roja continua representa la curva característica del ataque para cada uno de los grupos de nodos, según el modelo SIRD propuesto para este experimento. Los círculos azules representan los datos de referencia. Los trazos de línea gris claro representan cada una de las 300 realizaciones de *bootstrapping* obtenidas mediante la estructura de error basada en la distribución de *Poisson*

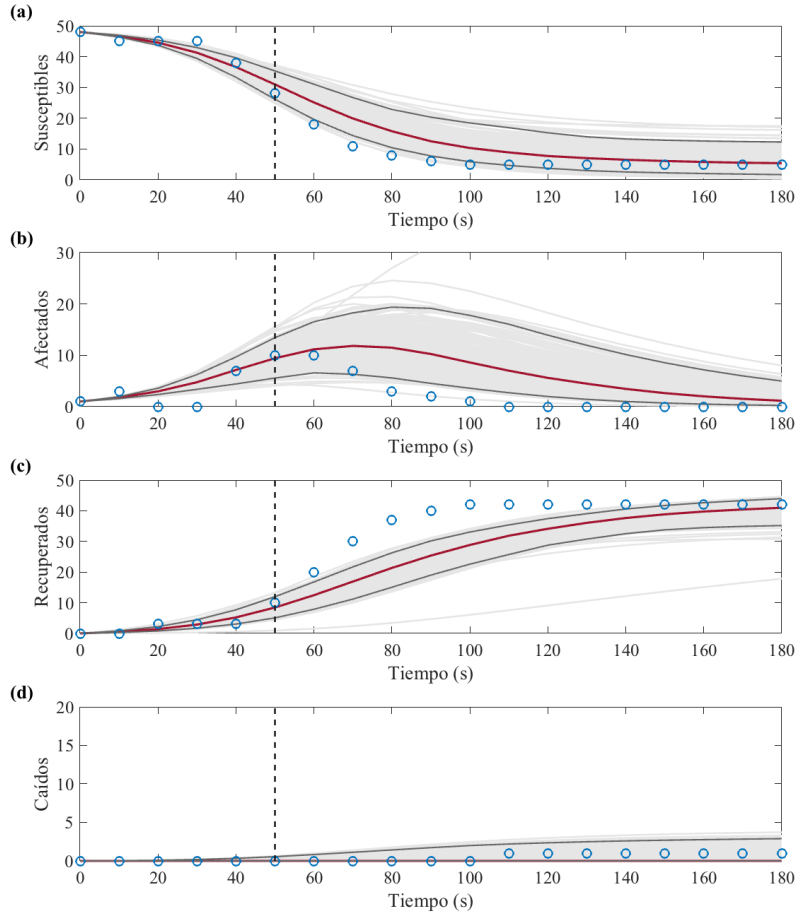


Figura A.III.2.4.

Curva de incidencia acumulada según modelo, (línea continua roja), intervalo de confianza al 95% (líneas grises), e incidencia acumulada de los datos de referencia (línea continua azul).

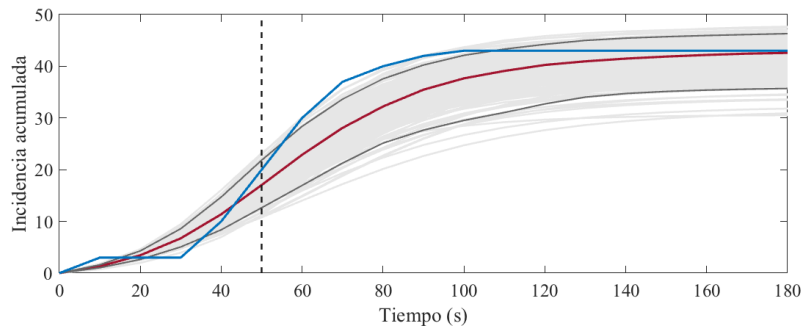
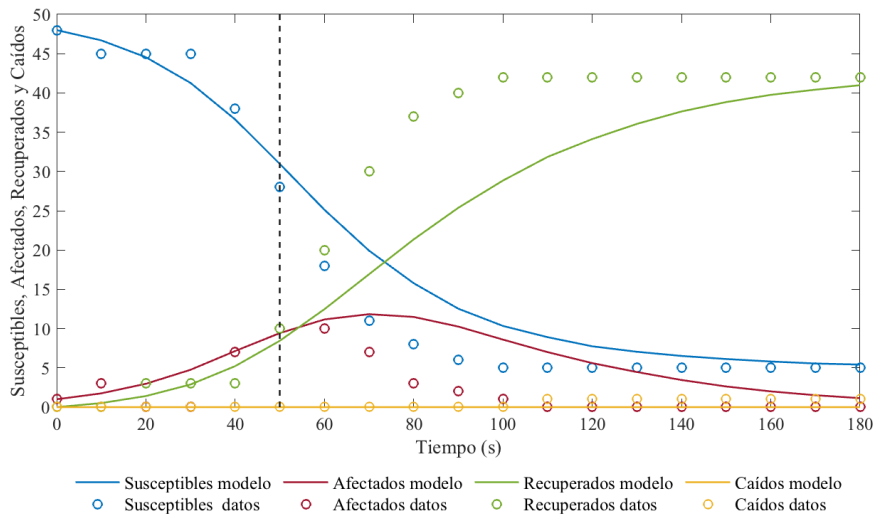


Figura A.III.2.5.

Comparativa de los resultados experimentales obtenidos por el modelo propuesto (trazos de línea continua coloreada), con respecto a los datos de referencia, (los círculos).



A.III.2.2 Estudio predictivo de propagación de ataques mediante el modelo epidémico SIR determinista. Caso de *jamming* aleatorio 50 p/s contra MPH. Tercer escenario de ataque con nodo atacante alejado del nodo coordinador de red.

Figura A.III.2.6.

Las gráficas (a), (b), (c) y (d) muestran el mejor ajuste inicial del modelo en la etapa temprana del ataque, para cada una de las curvas $dS(t)/dt$, $dI(t)/dt$, $dR(t)/dt$ y $dD(t)/dt$. La línea roja continua representa la curva característica del ataque para cada uno de los grupos de nodos, según el modelo SIRD propuesto para este experimento. Los círculos azules representan los datos de referencia. En misma figura, las gráficas (e), (f), (g) y (h) muestra los residuos en función del tiempo.

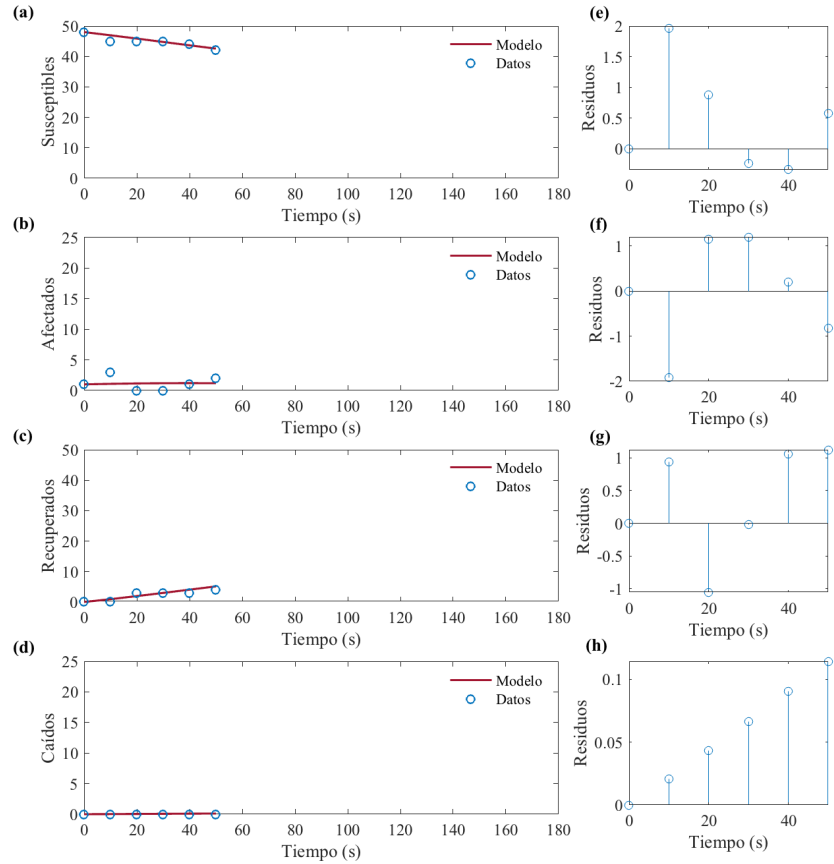


Figura A.III.2.7.

Histogramas con los valores del 95% del intervalo de confianza obtenido para los parámetros β , γ , y ν , gráficas (a), (b) y (c), respectivamente. El histograma (d) representa el intervalo de confianza estimado al 95% del número reproductivo básico \mathcal{R}_0 .

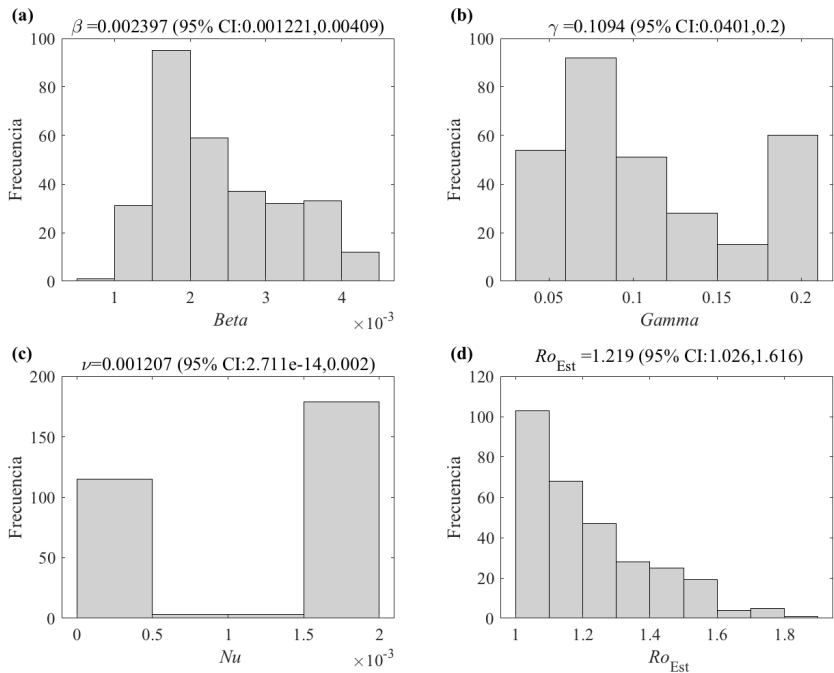


Figura A.III.2.8.

Las gráficas (a), (b), (c) y (d) muestran el mejor ajuste del modelo para cada una de las curvas $dS(t)/dt$, $dI(t)/dt$, $dR(t)/dt$ y $dD(t)/dt$. La línea roja continua representa la curva característica del ataque para cada uno de los grupos de nodos, según el modelo SIRD propuesto para este experimento. Los círculos azules representan los datos de referencia. Los trazos de línea gris claro representan cada una de las 300 realizaciones de *bootstrapping* obtenidas mediante la estructura de error basada en la distribución de *Poisson*

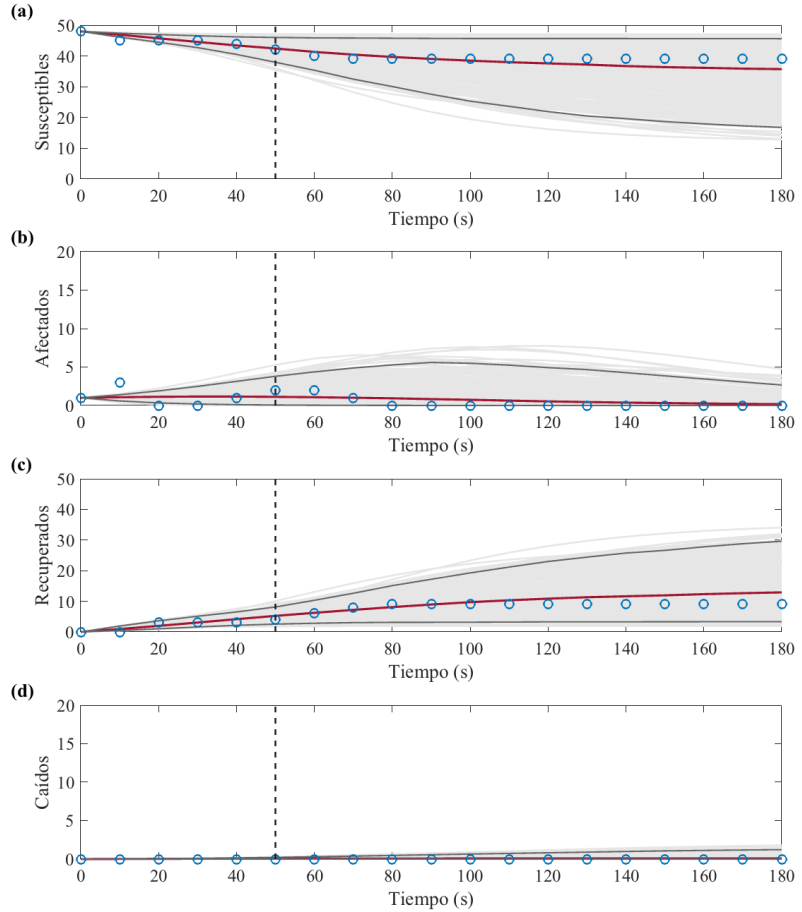


Figura A.III.2.9.

Curva de incidencia acumulada según modelo, (línea continua roja), intervalo de confianza al 95% (líneas grises), e incidencia acumulada de los datos de referencia (línea continua azul).

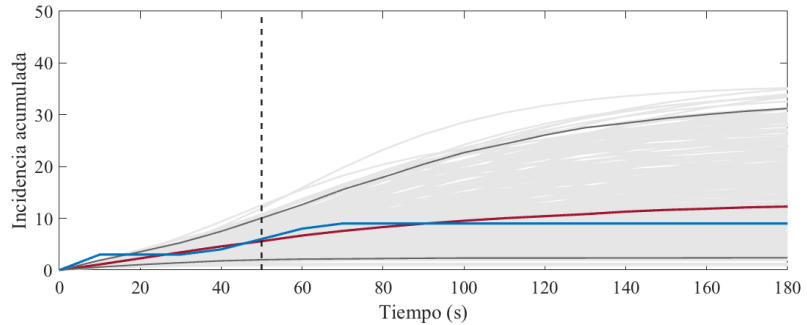
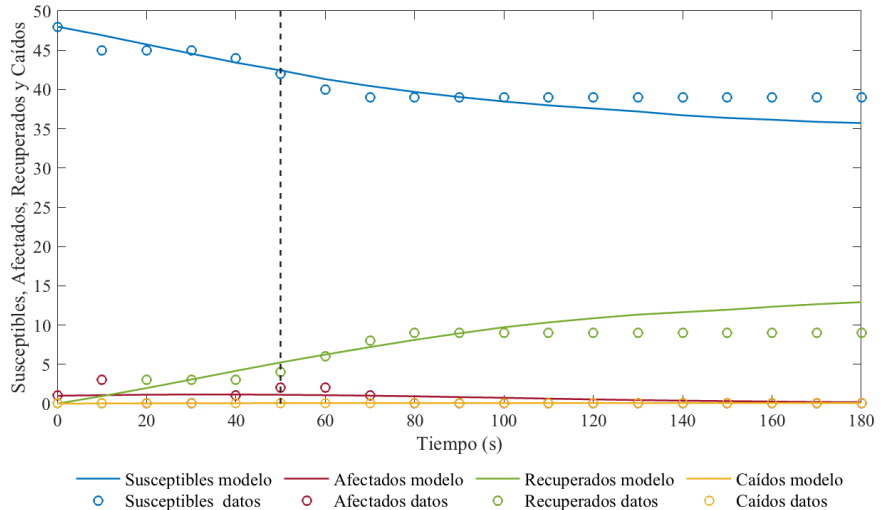


Figura A.III.2.10.

Comparativa de los resultados experimentales obtenidos por el modelo propuesto (trazos de línea continua coloreada), con respecto a los datos de referencia, (los círculos).



A.III.3.1 Estudio predictivo de propagación de ataques mediante el modelo epidémico de Crecimiento Generalizado GGM. Caso de *jamming* aleatorio a 80 p/s contra DSR. Primer escenario de ataque con nodo atacante próximo al nodo coordinador de red.

Figura A.III.3.1.

Mejor ajuste del modelo GGM para la fase inicial del ataque (a), donde la línea roja continua representa la curva característica del ataque, y los círculos azules representan los datos de referencia. En la misma figura, la gráfica (b) muestra los residuos en función del tiempo.

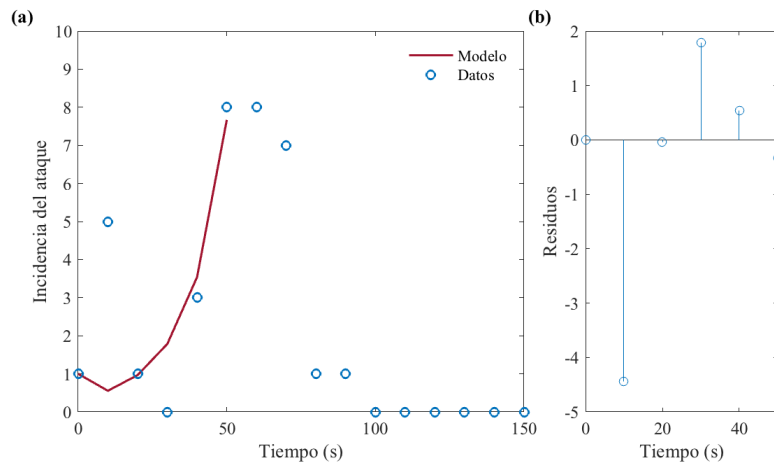


Figura A.III.3.2.

Histogramas de distribuciones empíricas para las estimaciones de parámetros r (a), y p (b) correspondientes al intervalo de confianza del 95%, y mejor ajuste de la curva de ataque (c), pronosticada en el experimento para el modelo GGM.

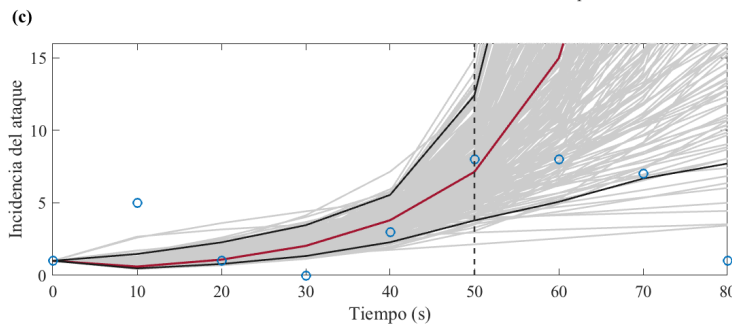
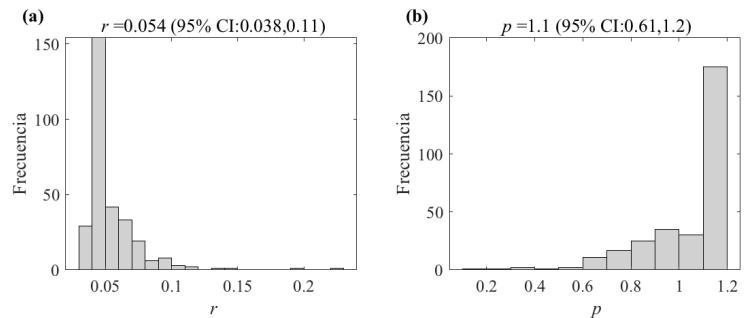
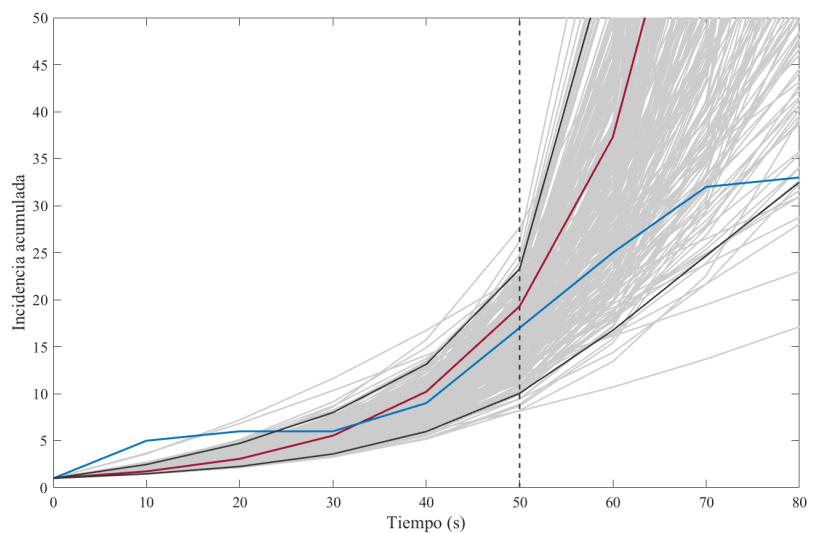


Figura A.III.3.3.

Mejor ajuste de la curva de nodos afectados acumulados $C(t)$ pronosticada por el modelo GGM.



A.III.3.2 Estudio predictivo de propagación de ataques mediante el modelo de Crecimiento Generalizado GGM. Caso de *jamming* reactivo contra MPH. Tercer escenario de ataque con nodo atacante alejado del nodo coordinador de red.

Figura A.III.3.4.

Mejor ajuste del modelo GGM para la fase inicial del ataque (a), donde la línea roja continua representa la curva característica del ataque, y los círculos azules representan los datos de referencia. En la misma figura, la gráfica (b) muestra los residuos en función del tiempo.

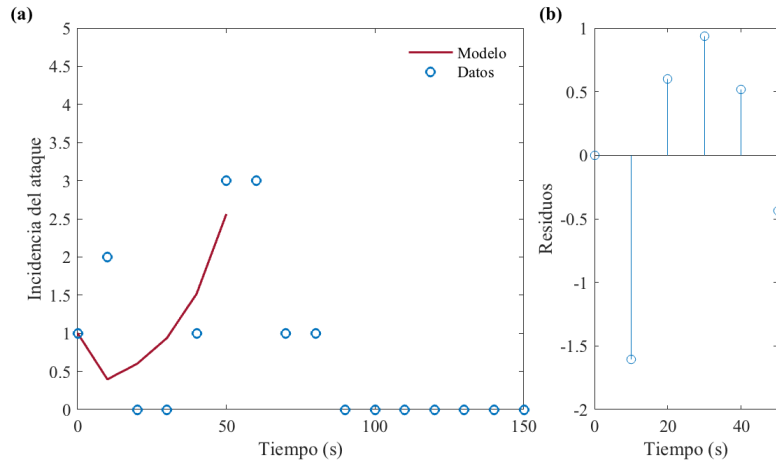


Figura A.III.3.5.

Histogramas de distribuciones empíricas para las estimaciones de parámetros r (a), y p (b) correspondientes al intervalo de confianza del 95%, y mejor ajuste de la curva de ataque (c), pronosticada en el experimento para el modelo GGM.

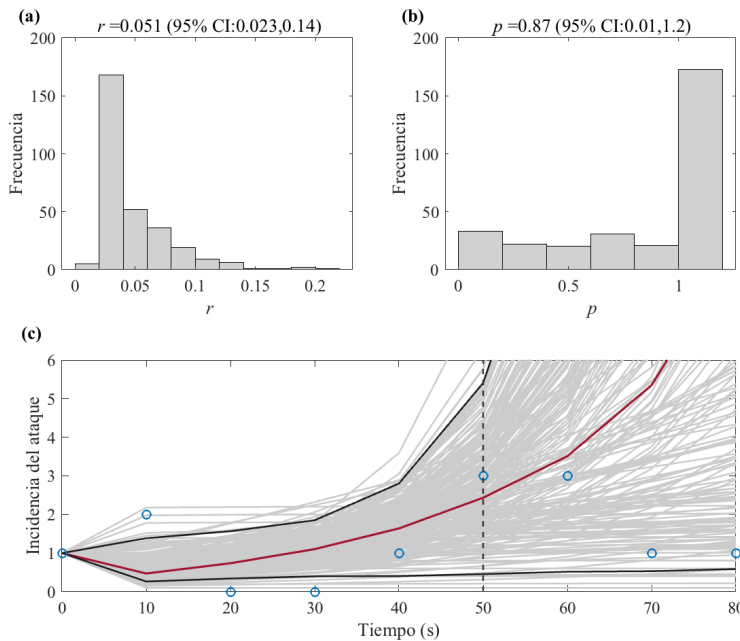
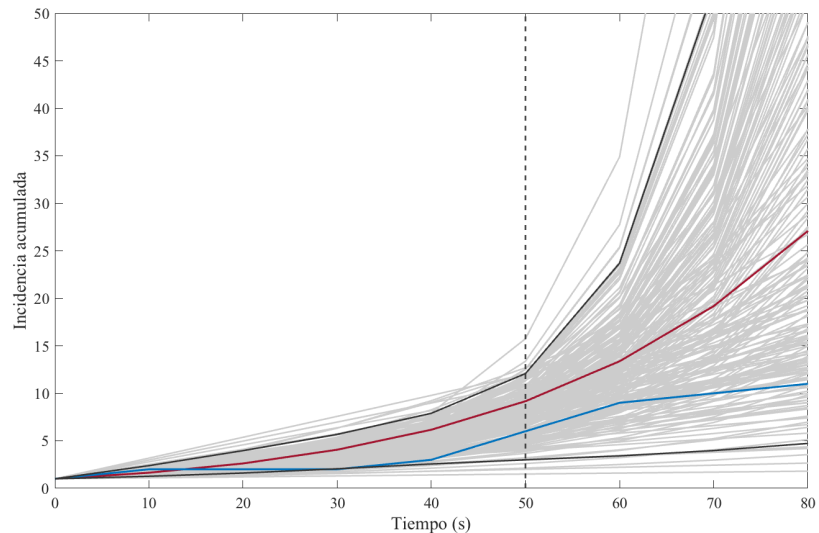


Figura A.III.3.6.

Mejor ajuste de la curva de nodos afectados acumulados $C(t)$ pronosticada por el modelo GGM.



A.III.4.1 Estudio predictivo de propagación de ataques mediante el modelo de Crecimiento Logístico Generalizado GLGM. Caso de *jamming* aleatorio a 80 p/s contra AODV. Segundo escenario de ataque con nodo atacante centrado en la topología de red.

Figura A.III.4.1.

Mejor ajuste del modelo GLGM para la fase inicial del ataque (a), donde la línea roja continua representa la curva característica del ataque, y los círculos azules representan los datos de referencia. En la misma figura, la gráfica (b) muestra los residuos en función del tiempo.

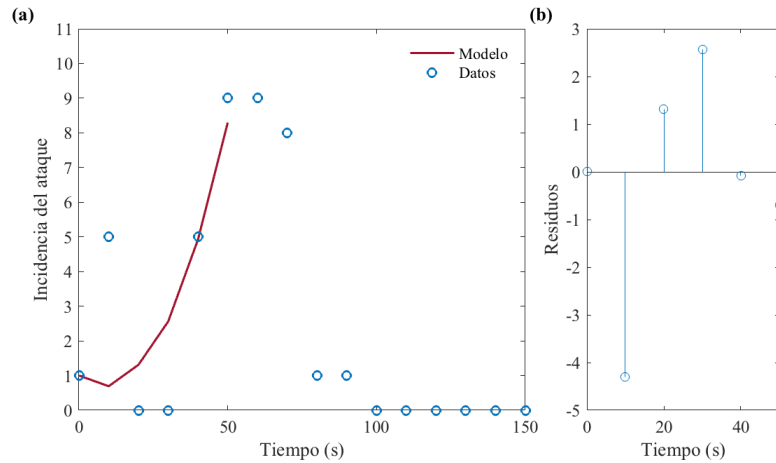


Figura A.III.4.2.

Histogramas de distribuciones empíricas para las estimaciones de parámetros r (a), p (b) y K (c), correspondientes al intervalo de confianza del 95%, y mejor ajuste de la curva de ataque (d), pronosticada en el experimento para el modelo GLGM.

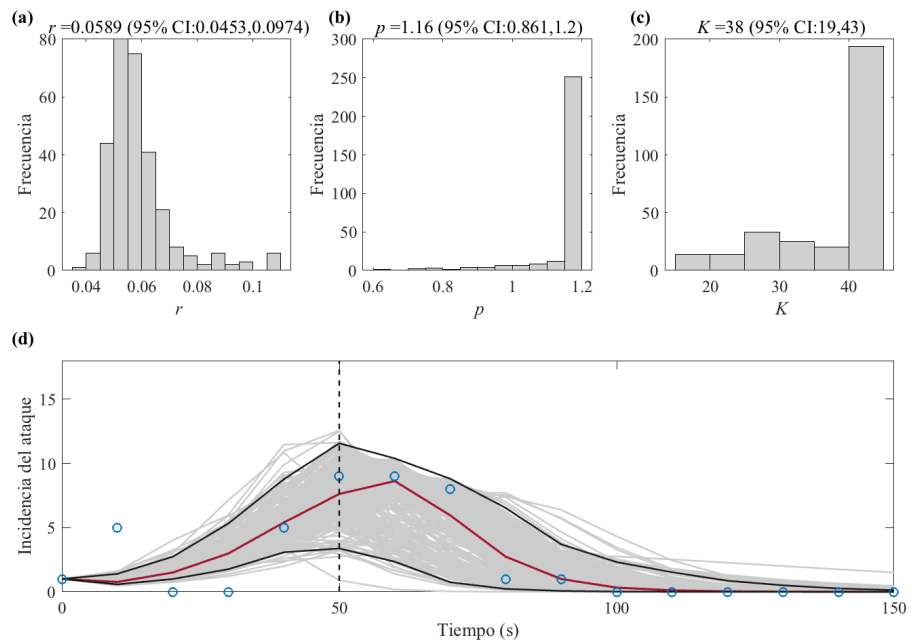
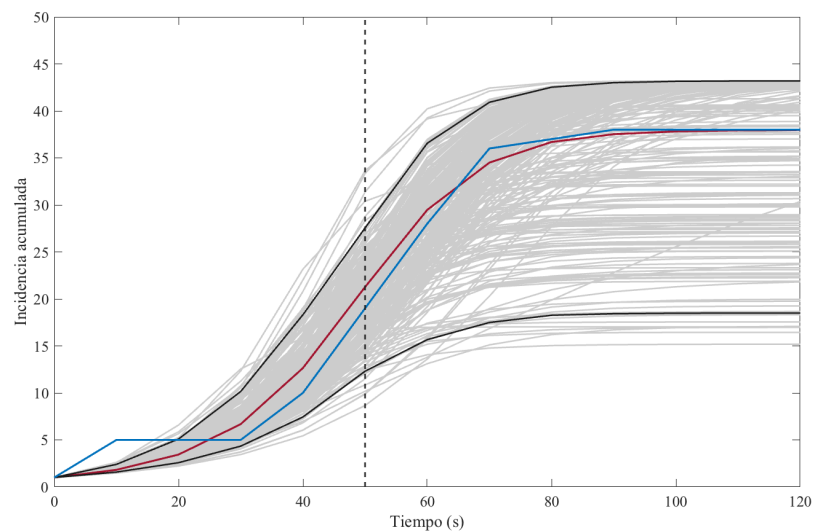


Figura A.III.4.3.

Mejor ajuste de la curva $C(t)$ pronosticada por el modelo GLGM.



A.III.4.2 Estudio predictivo de propagación de ataques mediante el modelo de Crecimiento Logístico Generalizado GLGM. Caso de *jamming* reactivo contra AODV. Tercer escenario de ataque con nodo atacante alejado del nodo coordinador de red.

Figura A.III.4.4.

Mejor ajuste del modelo GLGM para la fase inicial del ataque (a), donde la línea roja continua representa la curva característica del ataque, y los círculos azules representan los datos de referencia. En la misma figura, la gráfica (b) muestra los residuos en función del tiempo.

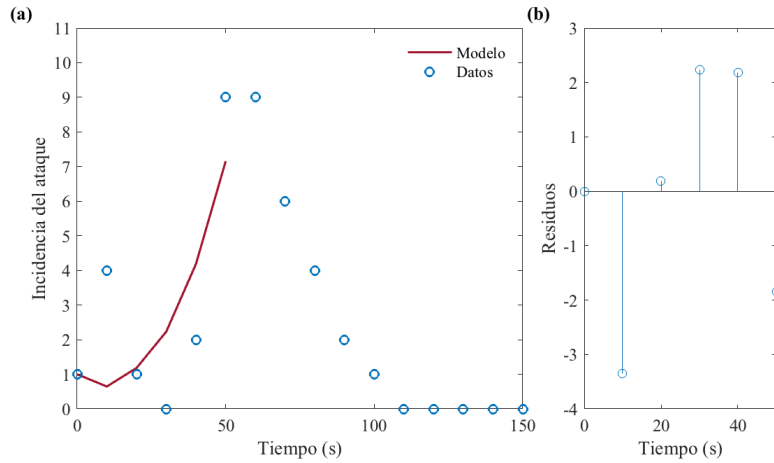


Figura A.III.4.5.

Histogramas de distribuciones empíricas para las estimaciones de parámetros r (a), p (b) y K (c), correspondientes al intervalo de confianza del 95%, y mejor ajuste de la curva de ataque (d), pronosticada en el experimento para el modelo GLGM.

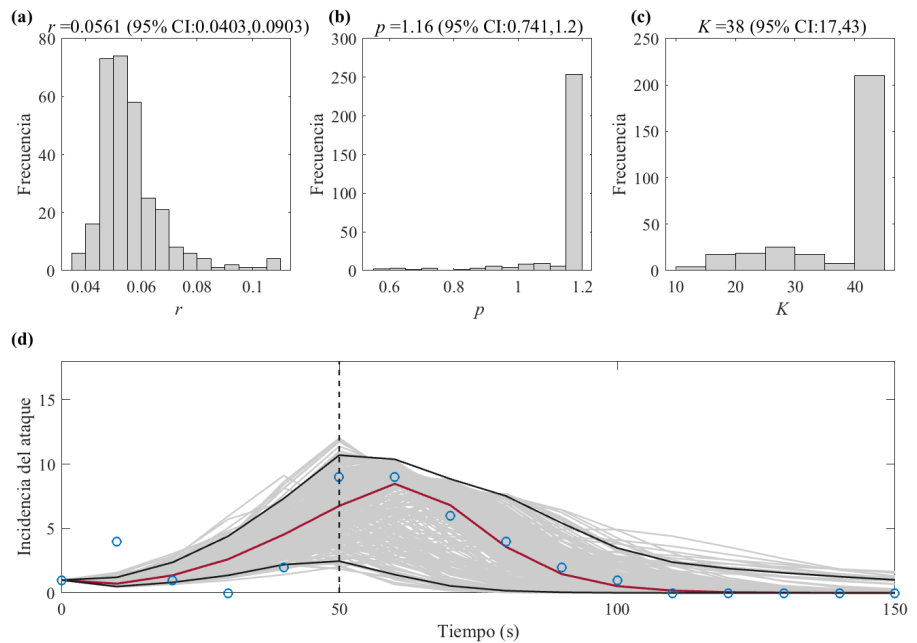
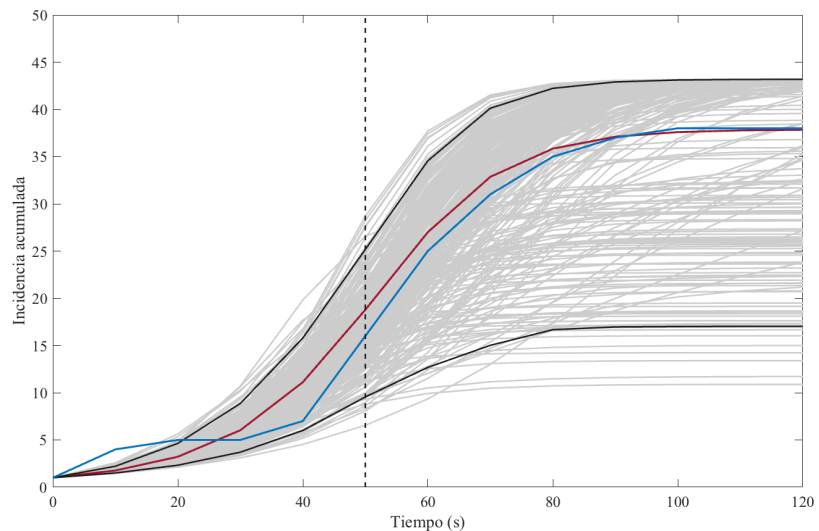


Figura A.III.4.6.

Mejor ajuste de la curva $C(t)$ pronosticada por el modelo GLGM.



A.III.5.1 Análisis de resultados de los experimentos del estudio retrospectivo de la propagación de ataques *jamming* mediante el modelo epidémico SIR determinista. Primer escenario de ataque con nodo atacante próximo al nodo coordinador de red.

Figura A.III.5.1.

Histogramas comparativos de la incidencia acumulada (a) y número de nodos supervivientes o dimensión del ataque (b), para los casos de *jamming* aleatorio y reactivo, según cada protocolo.

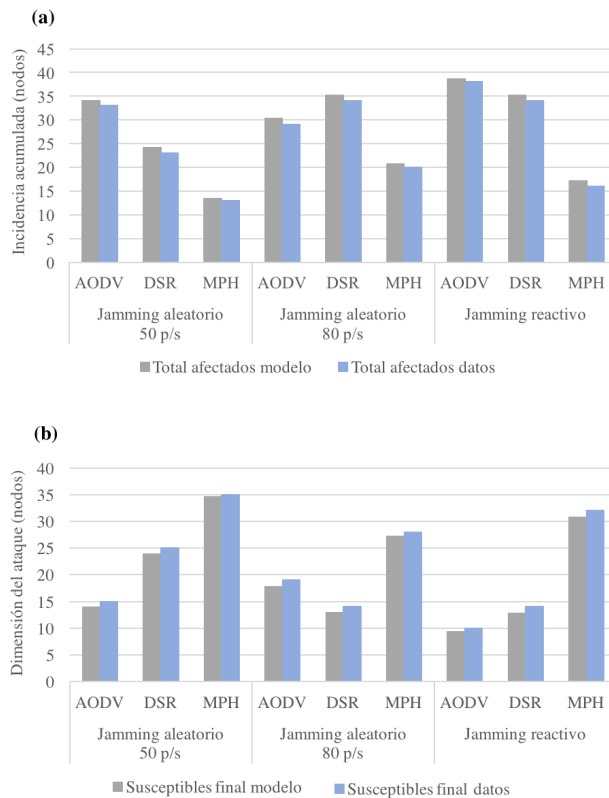


Figura A.III.5.2.

Histogramas comparativos de la severidad del ataque \mathcal{R}_0 , para los casos de *jamming* aleatorio y reactivo, según cada protocolo.

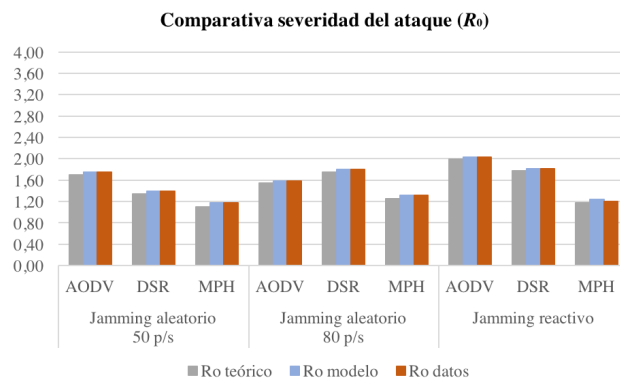
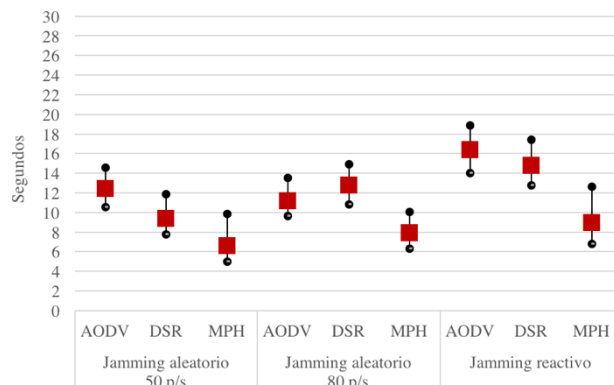


Figura A.III.5.3.

Comparativa de la persistencia del ataque, factor $1/\gamma$, para los casos de *jamming* aleatorio y reactivo, según cada protocolo.



A.III.5.2 Análisis de resultados de los experimentos del estudio retrospectivo de la propagación de ataques *jamming* mediante el modelo epidémico SIR determinista. Segundo escenario de ataque con nodo atacante centrado en la topología de red.

Figura A.III.5.4.

Histogramas comparativos de la incidencia acumulada (a) y número de nodos supervivientes o dimensión del ataque (b), para los casos de *jamming* aleatorio y reactivo, según cada protocolo.

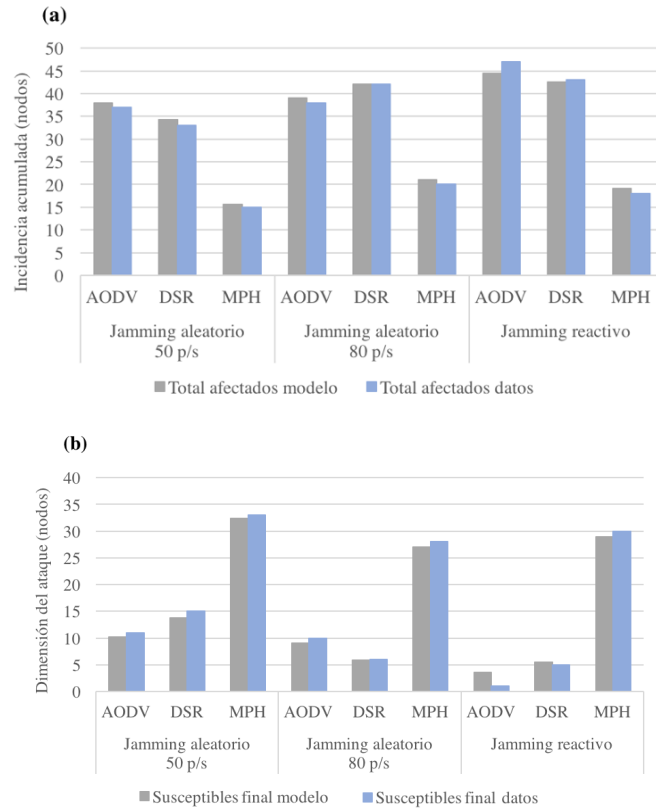


Figura A.III.5.5.

Histogramas comparativos de la severidad del ataque \mathcal{R}_0 , para los casos de *jamming* aleatorio y reactivo, según cada protocolo.

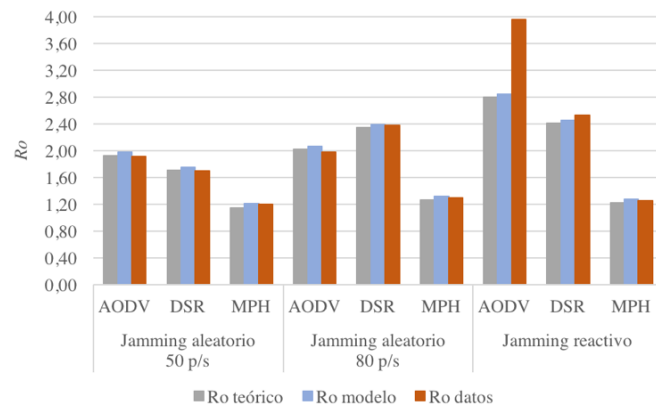
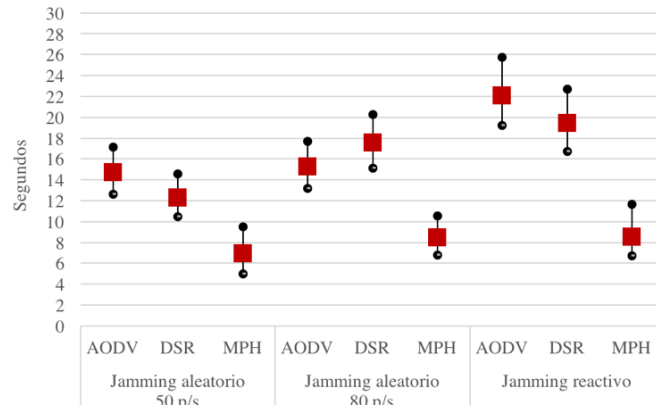


Figura A.III.5.6.

Comparativa de la persistencia del ataque, factor $1/\gamma$, para los casos de *jamming* aleatorio y reactivo, según cada protocolo.



A.III.5.3 Análisis de resultados de los experimentos del estudio retrospectivo de la propagación de ataques *jamming* mediante el modelo epidémico SIR determinista. Tercer escenario de ataque con nodo atacante alejado del nodo coordinador de red.

Figura A.III.5.7.

Histogramas comparativos de la incidencia acumulada (a) y número de nodos supervivientes o dimensión del ataque (b), para los casos de *jamming* aleatorio y reactivo, según cada protocolo.

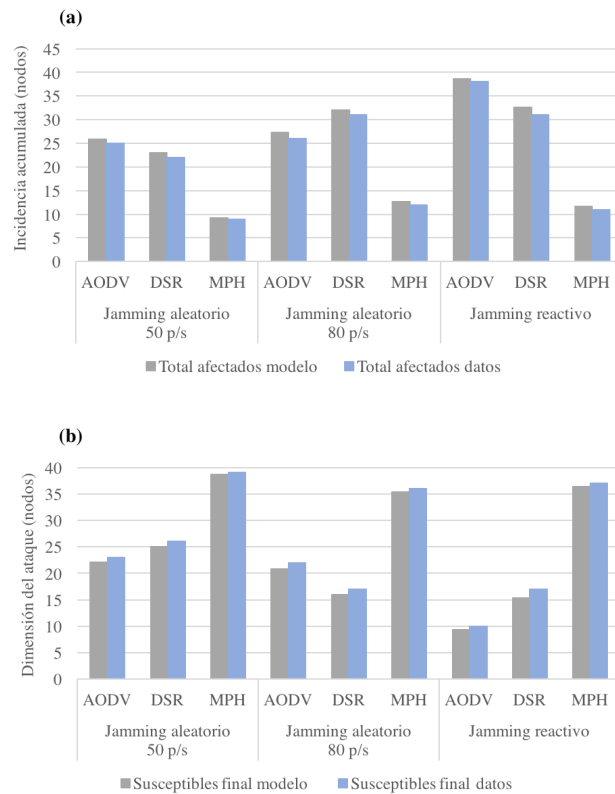


Figura A.III.5.8.

Histogramas comparativos de la severidad del ataque R_0 , para los casos de *jamming* aleatorio y reactivo, según cada protocolo.

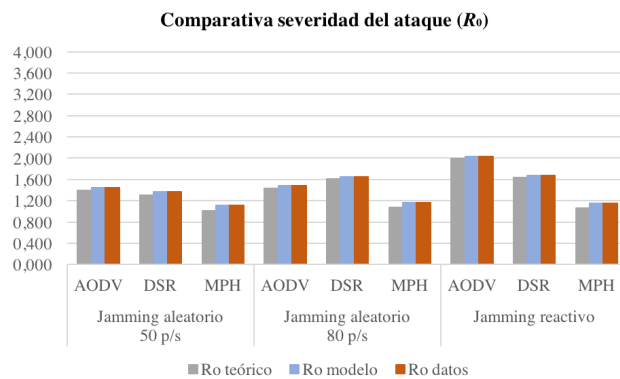
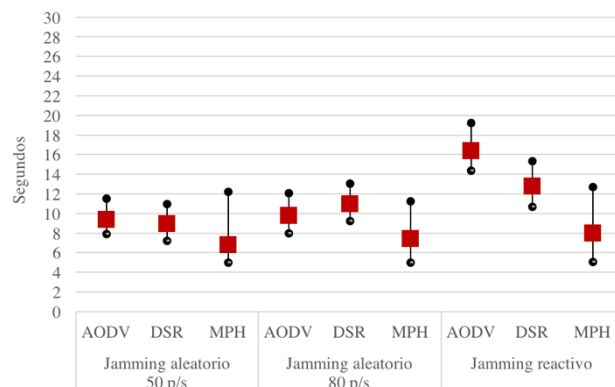


Figura A.III.5.9.

Comparativa de la persistencia del ataque, factor $1/\gamma$, para los casos de *jamming* aleatorio y reactivo, según cada protocolo.



A.III.6.1 Análisis de resultados de los experimentos del estudio predictivo de propagación de ataques mediante el modelo de Crecimiento Logístico Generalizado GLGM. Primer escenario de ataque con nodo atacante próximo al nodo coordinador de red.

Figura A.III.6.1.

Comparativa de resultados pronosticados por GLGM de la evolución de nodos afectados para los casos de *jamming* aleatorio y reactivo, según cada protocolo, a los 50 segundos (a) y a los 60 segundos (b).

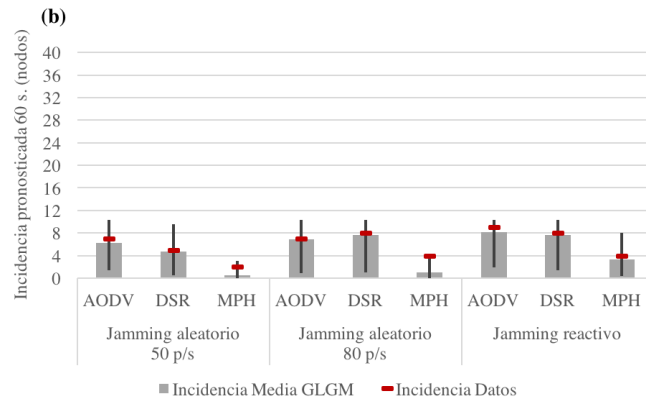
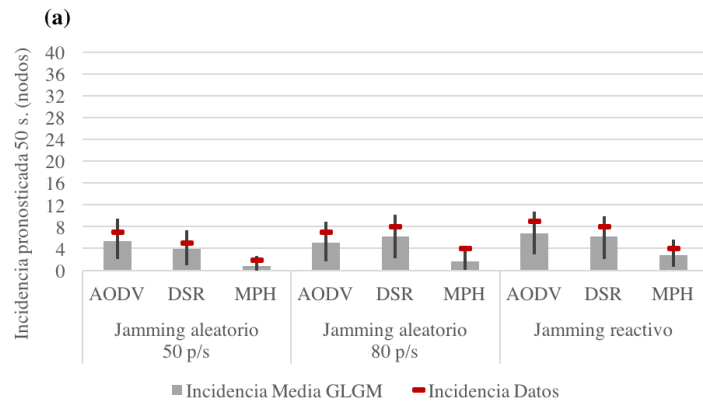
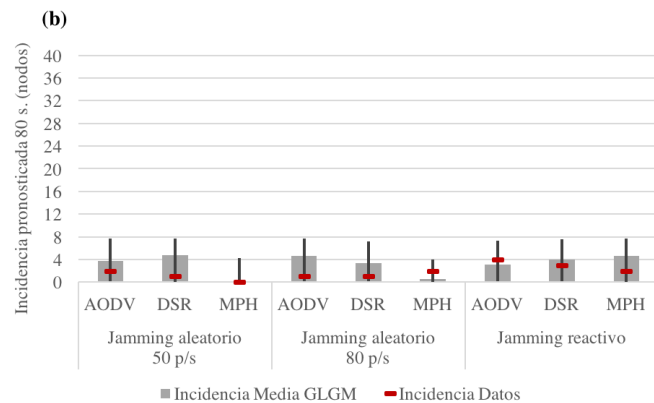
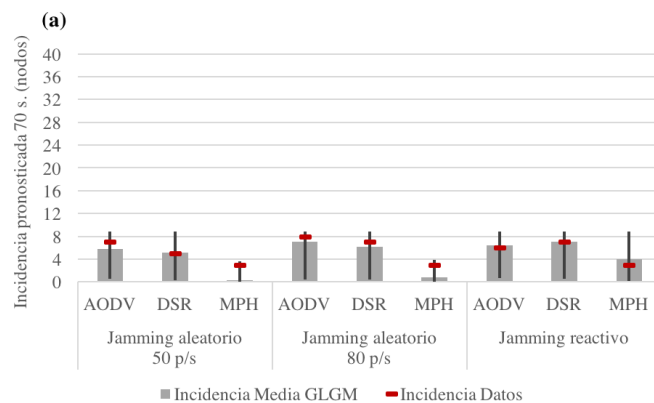


Figura A.III.6.2.

Comparativa de resultados pronosticados por GLGM de la evolución de nodos afectados para los casos de *jamming* aleatorio y reactivo, según cada protocolo, a los 70 segundos (a) y a los 80 segundos (b).



A.III.6.2 Análisis de resultados de los experimentos del estudio predictivo de propagación de ataques mediante el modelo de Crecimiento Logístico Generalizado GLGM. Segundo escenario de ataque con nodo atacante centrado en la topología de red.

Figura A.III.6.3.

Comparativa de resultados pronosticados por GLGM de la evolución de nodos afectados para los casos de *jamming* aleatorio y reactivo, según cada protocolo, a los 50 segundos (a) y a los 60 segundos (b).

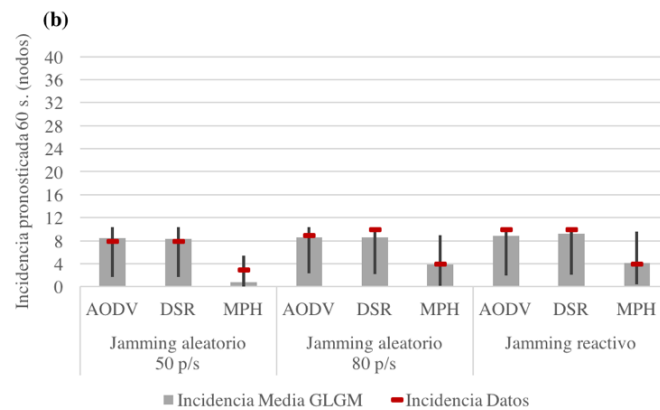
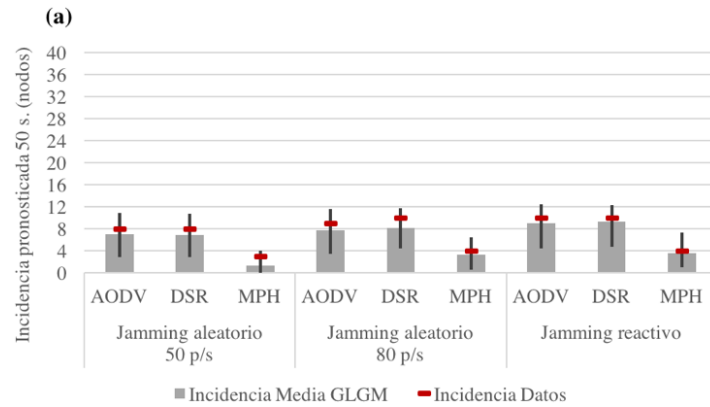
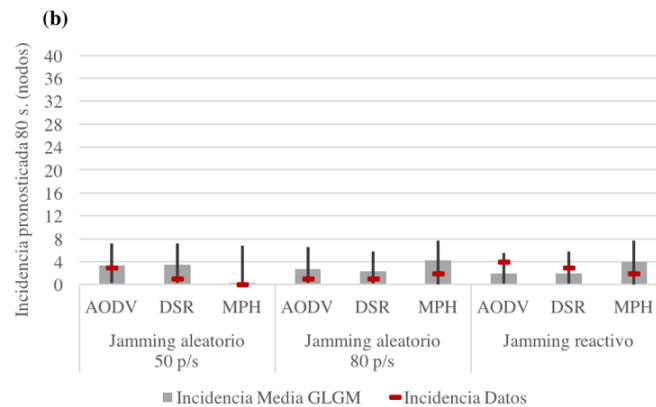
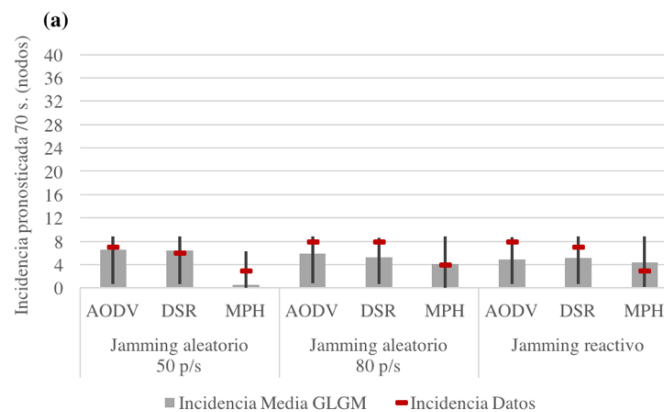


Figura A.III.6.4.

Comparativa de resultados pronosticados por GLGM de la evolución de nodos afectados para los casos de *jamming* aleatorio y reactivo, según cada protocolo, a los 70 segundos (a) y a los 80 segundos (b).



A.III.6.3 Análisis de resultados de los experimentos del estudio predictivo de propagación de ataques mediante el modelo de Crecimiento Logístico Generalizado GLGM. Tercer escenario de ataque con nodo atacante alejado del nodo coordinador de red.

Figura A.III.6.5.

Comparativa de resultados pronosticados por GLGM de la evolución de nodos afectados para los casos de *jamming* aleatorio y reactivo, según cada protocolo, a los 50 segundos (a) y a los 60 segundos (b).

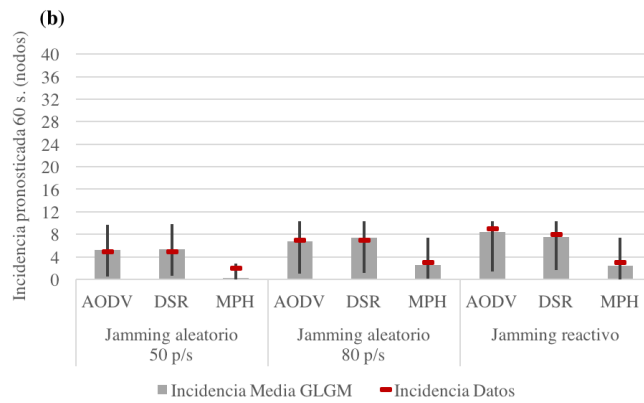
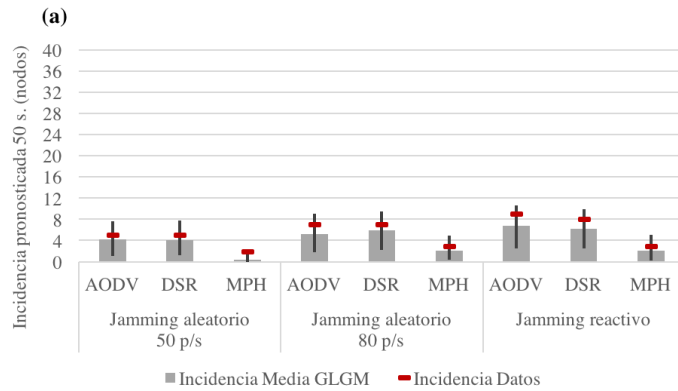
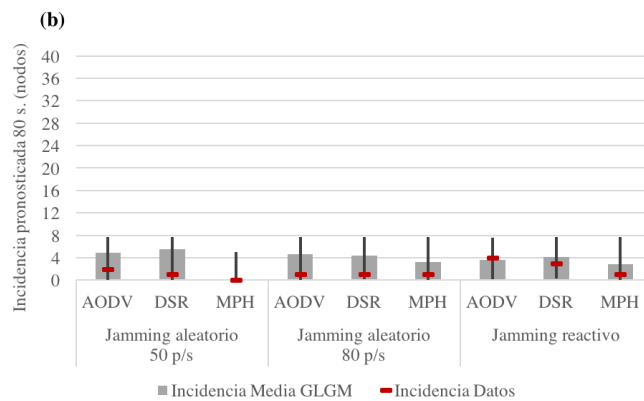
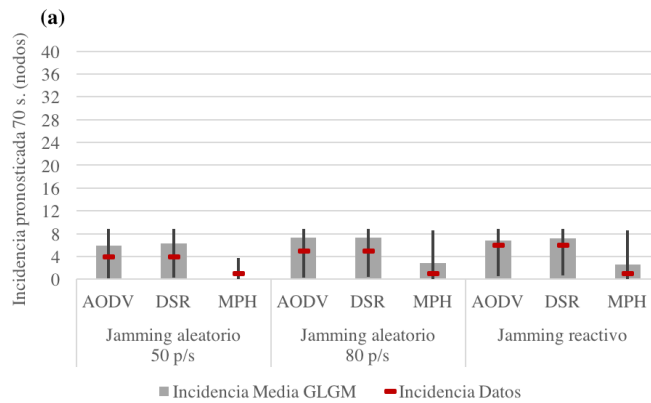


Figura A.III.6.6.

Comparativa de resultados pronosticados por GLGM de la evolución de nodos afectados para los casos de *jamming* aleatorio y reactivo, según cada protocolo, a los 70 segundos (a) y a los 80 segundos (b).



REFERENCIAS

- [1] Eubank, S., Anil Kumar, A., Marathe, M. *Epidemiology and Wireless Communication: Tight Analogy or Loose Metaphor?* LNCS 5151, pp. 91–104, Springer-Verlag 2008.
- [2] Kephart, J.O., White, S.R. *Directed-graph epidemiological models of computer viruses*. IEEE Symposium on Security and Privacy, pp. 343–359, IEEE 1991.
- [3] De, P., Liu, Y., Das, S. K., *An Epidemic Theoretic Framework for Vulnerability Analysis of Broadcast Protocols in Wireless Sensor Networks*. IEEE Transactions on Mobile Computing, vol. 8, n° 3, pp. 413–425. IEEE 2009.
- [4] Tang, S. *A Modified SI Epidemic Model for Combating Virus Spread in Wireless Sensor Networks*. International Journal Wireless Information Networks, 18, pp. 319–326. IEEE 2011.
- [5] Di Pietro, R., Verde, N. V. *Epidemic theory and data survivability in unattended wireless sensor networks: Models and gaps*. Pervasive & Mobile Computing, vol. 9, pp. 588–597. ACM 2013.
- [6] Mishra, B. K., Mishra, B. K. *A quarantine model on the spreading behavior of worms in wireless sensor network*. Transaction on IoT and Cloud Computing, vol 2, pp. 1–12. 2014.
- [7] Zhu, L., Zhao, H. *Dynamical Analysis and Optimal control for a malware propagation model in an information network*. Neurocomputing, vol. 149, pp. 1370–1386, ScienceDirect 2015.
- [8] Chukwu Nonso H., Nwokoye, Onyesolu, M. O. *Modeling Multigroup Malicious Code Infections in Sensor Networks*. International Journal of Control and Automation, vol. 11, n° 3, pp. 129–142. Springer 2018.
- [9] Srivastava, P.K., Sharma, K., Awasthi, S., Sanyal, G. Ojha, P. R. *Effect of Quarantine and Recovery on infectious nodes in Wireless Sensor Network*. International Journal of Sensors, Wireless Communications and Control vol. 08, pp. 26–36. Bentham Sc. 2018.

- [10] Mishra, B. K., Keshri, A. K., Mallick, D. K., Mishra, B. K. *Mathematical model on distributed denial of service attack through Internet of things in a network*. Nonlinear Engineering, vol. 8, pp. 486–495. Published Online 2018.
- [11] *Mirai Botnet*. The New Jersey Cybersecurity and Communications Integration Cell. NJCCIC 2016. Accesible online: <https://www.cyber.nj.gov/threat-profiles/botnet-variants/mirai-botnet>
- [12] Lanz, A., Rogers, D., Alford, T. L. *An Epidemic Model of Malware Virus with Quarantine*. Journal of Advances in Mathematics and Computer Science, vol. 33, issue 8, pp. 1–10. 2019
- [13] Biswal, S.R., Swain, S. K. *Analyze The Effects of Quarantine And Vaccination on Malware Propagation in Wireless Sensor Network*. International Journal of Innovative Technology and Exploring Engineering, vol. 8, issue 10, pp. 3537–3543. 2019.
- [14] Zhang, Z., Kundu, S., Wei, R. *A Delayed Epidemic Model for Propagation of Malicious Codes in Wireless Sensor Network*. Mathematics vol. 7, issue 5, pp. 1–18. MDPI 2019.
- [15] *ISO/IEC 7498-4:1989 Information technology, Open Systems Interconnection, Basic Reference Model: Naming and addressing*. Acceso online <http://standards.iso.org/ittf/PubliclyAvailableStandards/>
- [16] Dressler, F., Akanb, O. B. *A Survey on Bio-inspired Networking*. Computer Networks vol. 54, issue 6, pp. 881–900. Elsevier 2010.
- [17] M. López, A. Peinado, A. Ortiz. *Modelo epidemiológico para el estudio de los ataques tipo jamming en redes de sensores inalámbricos*. JNIC2016, Sesión 1: Seguridad Industrial, Infraestructuras Críticas. 2016.
- [18] M. López, A. Peinado, A. Ortiz. *A SEIS Model for Propagation of Random Jamming Attacks in Wireless Sensor Networks*. International Joint Conference SOCO'16-CISIS'16-ICEUTE'16. 2016.
- [19] M. López, A. Peinado, A. Ortiz. *Modelo epidemiológico para la propagación del jamming aleatorio en redes de sensores inalámbricos*. XIV Reunión Española sobre Criptología y Seguridad de la Información, RECSI 2016. Octubre 2016.
- [20] M. López, A. Peinado, A. Ortiz. *Validation of a SIR Epidemic Model for the Propagation of Jamming Attacks in Wireless Sensor Networks*. XV Reunión Española sobre Criptología y Seguridad de la Información, sesión 5, IoT y SmartGrid 2018.

- [21] M. López, A. Peinado, A. Ortiz. *An extensive validation of a SIR epidemic model to study the propagation of jamming attacks against IoT wireless networks*. Computer Networks, vol. 165, issue 24. Elsevier B.V. 2019.
- [22] Del Valle-Soto, C., Mex-Perera, C., Monroy, R. and Nolazco-Flores, J. *On the Routing Protocol Influence on the Resilience of Wireless Sensor Networks to Jamming Attacks*. Sensors, vol. 15, pp. 7619–7649, 2015.
- [23] López, M. *On the Effectiveness of Intrusion Detection Strategies for Wireless Sensor Networks: An Evolutionary Game Approach*. Ad Hoc & Sensor Wireless Networks, vol. 35, pp. 25–40. Old City Publishing, Inc. 2017.
- [24] M. López, A. Peinado, A. Ortiz. *Characterizing two outbreak waves of COVID-19 in Spain using phenomenological epidemic modelling*. PLOS ONE 2021. <https://doi.org/10.1371/journal.pone.0253004>
- [25] Gupta, C.P., Kumar, A. *Wireless Sensor Networks: A Review*. International Journal of Sensors Wireless Communications and Control, vol. 3, pp. 25–36, 2013.
- [26] Murti, K. *Design Principles for Embedded Systems*. Transactions on Computer Systems and Networks, pp. 391–417, Springer Nature 2022.
- [27] Karray, F., Jmal, M., Garcia-Ortiz, A., Abid, M., Obeid, A. *A comprehensive survey on wireless sensor node hardware platforms*. Computer Networks, vol. 144, pp. 89–110. Elsevier 2018.
- [28] Jondhale, S. R., Maheswar, R., Lloret, J. *Received Signal Strength Based Target Localization and Tracking Using Wireless Sensor Networks*. Springer Innovations in Communication and Computing, pp. 1–18, Springer Nature 2022.
- [29] Ouadjaout, A., Minéc, A., Noureddine, L., Badache, N. *Static analysis by abstract interpretation of functional properties of device drivers in TinyOS*. The Journal of Systems and Software, vol. 120, pp. 114–132. Elsevier 2016.
- [30] Dunkels, A., Gronvall, B., Voigt, T. *Contiki a lightweight and flexible operating system for tiny networked sensors*. In. proc. 29th annual IEEE International Conference on Local Computer Networks, pp. 455–462. IEEE 2004.
- [31] Baccelli, E., Hahm, O., Gunes, M., Wahlisch, M., Schmidt, T.C. *RIOT OS: towards an OS for the internet of things*. In. proc. IEEE Conference on Computer Communications Workshops, pp. 79–80. IEEE 2013.
- [32] <https://developer.android.com/things/index.html>
- [33] <https://www.ti.com/product/CC2420>

- [34] <https://csa-iot.org/all-solutions/zigbee/>
- [35] *ZigBee Specification*. Revision 22 1.0, Document 05-3474-22. Zigbee Alliance 2017.
- [36] Mohamed, R.E., Saleh, A.I., Abdelrazzak, M. *Survey on Wireless Sensor Network Applications and Energy Efficient Routing Protocols*. *Wireless Personal Communications*, n° 101, pp. 1019–1055. Springer 2018.
- [37] Karapistoli, E., Mampentzidou, I., Economides, A. *Environmental Monitoring Based on the Wireless Sensor Networking Technology: A Survey of Real-World Applications*. *Mobile Computing and Wireless Networks: Concepts, Methodologies, Tools, and Applications*, pp. 1332-1374. IGI Global 2016.
- [38] Kandris, D., Nakas, C., Vomvas, D., Koulouras, G. *Applications of Wireless Sensor Networks: An Up-to-Date Survey*. *Applied Systems Innovation*, vol. 3. MDPI Journals 2020.
- [39] Fahmy H.M.A. *WSN Applications*. Concepts, Applications, Experimentation and Analysis of Wireless Sensor Networks. *Signals and Communication Technology*, pp. 67–232. Springer 2019.
- [40] Aponte-Luis, J., Gómez-Galán, J. A., Gómez-Bravo, F., Sánchez-Raya, M., Alcina-Espigado, J., Teixido-Rovira, M. *An Efficient Wireless Sensor Network for Industrial Monitoring and Control*. *Sensors*, n°18, vol. 182. MDPI 2018.
- [41] Ketshabetswe, L. K., Zungeru, A. M., Mangwala, M., Chuma, J. M., Sigweni, B. *Communication protocols for wireless sensor networks: A survey and comparison*. *Heliyon*, vol. 5. Elsevier 2019.
- [42] Day, J. D., Zimmermann, H. *The OSI Reference Model*. In proceedings of the IEEE vol. 71, n°. 12, pp. 1334–1340. IEEE 1983.
- [43] Goralski, W. *The Illustrated Network. How TCP/IP Works in a Modern Network*. Morgan Kaufmann - Elsevier 2009.
- [44] 802.15.4-2020 - *IEEE Approved Draft Standard for Low-Rate Wireless Networks*. IEEE 2020. https://standards.ieee.org/standard/802_15_4-2020.html
- [45] Coboi, A., Van-Cuong N., Minh, N., Thang, T. *An Analysis of ZigBee Technologies for Data Routing in Wireless Sensor Networks*. *ICSES Transactions on Computer Networks and Communications (ITCNC)*, vol. X, n°. Y. ICSES 2021.
- [46] IEC 62591:2016 *Industrial networks - Wireless communication network and communication profiles – WirelessHART*. <https://webstore.iec.ch/publication/24433>
- [47] ANSI/ISA-100.11a-2011 *Wireless systems for industrial automation: Process control and related applications*. International Society of Automation 2011.

- [48] *IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN)*. Internet Engineering Task Force (IETF) 2017. <https://datatracker.ietf.org/wg/6lowpan/charter/>
- [49] LoRaWAN, Low Power Wide Area Network, <https://lora-alliance.org>
- [50] Du, W., Navarro, D., Mieleville, F. *Performance evaluation of IEEE 802.15.4 sensor networks in industrial applications*. International Journal of Communication Systems, 2015, vol. 28, n° 10, pp. 1657–1674. John Wiley & Sons 2015.
- [51] *IEEE Standard for Low-Rate Wireless Networks Amendment 3: Advanced Encryption Standard AES256 Encryption and Security Extensions*. IEEE 802.15.4y 2021.
- [52] Kochhar, A., Kaur, P., Singh, P., & Sharma, S. *Protocols for wireless sensor networks: A survey*. Journal of Telecommunications and Information Technology, n° 1, pp. 1657–1674. 2018
- [53] Perkins, C., Royer, E. *Ad-hoc on-demand distance vector routing*. IEEE Workshop on Mobile Computing Systems and Applications, pp. 90–100. 1999.
- [54] Maltz, D., Broch, J., Jetcheva, J., Johnson, D. *The effects of on-demand behavior in routing protocols for multihop wireless ad hoc networks*. IEEE Journal Sel. Areas Communications, n° 17, pp. 1439–1453. 1999.
- [55] Del Valle-Soto C., Mex-Perera C., Olmedo O., Orozco-Lugo A., Galván-Tejada G., Lara M. *An efficient Multi-Parent Hierarchical Routing Protocol for WSNs*. Wireless Telecommunications Symposium, pp. 1–8. 2014.
- [56] Zhu, L., Zhao, H. *Dynamical Analysis and Optimal control for a malware propagation model in an information network*. Neurocomputing, Vol. 149, pp. 1370–1386, 2015.
- [57] Chukwu, H., Nwokoye, W., Onyesolu, M. *Modeling Multigroup Malicious Code Infections in Sensor Networks*. International Journal of Control and Automation Vol. 11, No. 3, pp.129–142, 2018.
- [58] Tayebi, A., Berber, S.M., Swain, A. *Wireless Sensor Network Attacks: An Overview and Critical Analysis with Detailed Investigation on Jamming Attack Effects*. Sensing Technology: Current Status and Future Trends III, Springer, 2015.
- [59] Diaz, A., Sanchez, P. *Simulation of Attacks for Security in Wireless Sensor Network*. Sensors Vol. 16, MDPI Journals, 2016.
- [60] Adepun, S., Prakash, J., Mathur, A. *WaterJam: An Experimental case study of Jamming Attacks on a Water Treatment System*. International Conference on Software Quality, Reliability and Security, pp. 341–347, IEEE 2017.

- [61] O'Mahony, G.D., Harris, P. J., Murphy, C. C. *Analyzing the Vulnerability of Wireless Sensor Networks to a Malicious Matched Protocol Attack*. International Carnahan Conference on Security Technology (ICCST), IEEE 2018.
- [62] Gavrić, Ž., Simić, D. *Overview of DOS attacks on wireless sensor networks and experimental results for simulation of interference attacks*. *Ingeniería e Investigación*, vol. 38 n.º 1, pp. 130–138, 2018.
- [63] Nafis, M. U., Fahmin, A., Hossain, S., Atiquzzaman, M. *Denial-of-Service Attacks on Wireless Sensor Network and Defense Techniques*. *Wireless Personal Communications*, Springer, 2020.
- [64] National Institute of Standards and Technology. Information Technology Laboratory. Computer Security Resource Center. <https://csrc.nist.gov/glossary/term/security>
- [65] Kardi, A., Zagrouba, R. *Attacks classification and security mechanisms in Wireless Sensor Networks*. *Advances in Science, Technology and Engineering Systems Journal*, vol. 4, pp. 229–243, 2019.
- [66] Singh, A. K., Patro, B.D.K. *Security Requirements and Attacks in Wireless Sensor Networks*. *International Journal of Applied Engineering Research* vol. 14, pp. 158–16, 2019.
- [67] Boubiche, D. E., Athmani, S. Boubiche, S, Toral-Cruz, H. *Cybersecurity Issues in Wireless Sensor Networks: Current Challenges and Solutions*. *Wireless Personal Communications*, Springer Nature, 2020.
- [68] Wood, A.D., Stankovic, J.A. *Denial of service in sensor networks*. *Computer*, vol. 35, pp. 54–62, IEEE, 2002.
- [69] Chen, X., Makki, K., Yen, K., Pissinou, N. *Sensor Network Security: A Survey*. *IEEE Communications Surveys Tutorials*, vol. 11, pp. 52–73, 2009.
- [70] Koubâa, A., Alves, M., Tovar, E. *IEEE 802.15.4 for Wireless Sensor Networks: A Technical Overview*. Technical Report, Polytechnic Institute of Porto, 2005.
- [71] Grover, J., Sharma, S. *Security Issues in Wireless Sensor Network – A Review*. *International Conference on Reliability, Infocom Technologies and Optimization*, pp. 397–404, IEEE 2016.
- [72] Ye, W., Heidemann, J., Estrin, D. *An energy-efficient MAC protocol for wireless sensor networks*. In *Proceedings of the twenty-first annual joint conference of the IEEE computer and communications societies*, pp. 1567–1576, IEEE 2002.

- [73] Rajkumar Vani B. A, Rajaraman, G., Chandrakanth, H. G. *Security Attacks and its Countermeasures in Wireless Sensor Networks*. Int. Journal of Engineering Research and Applications, vol. 4, pp. 04–15, 2014.
- [74] Chowdhury, M., Kader, M.F., Asaduzzaman. *Security Issues in Wireless Sensor Networks: A Survey*. International Journal of Future Generation Communication and Networking, vol. 6, pp. 97–116, 2013.
- [75] Chen, K., Zhang, S., Li, Z., Zhang, Y., Deng, Q., Ray, S., Jin, Y. *Internet-of-Things Security and Vulnerabilities: Taxonomy, Challenges, and Practice*. Journal of Hardware and Systems Security, pp. 97–110, Springer, 2018.
- [76] Jia, Y.J., Chen, Q.A., Wang, S., Rahmati, A., Fernandes, E., Mao, Z.M., Prakash, A. *ContextIoT: towards providing contextual integrity to appified IoT platforms*. In Proceedings of the 21st Network and Distributed System Security Symposium, 2017.
- [77] Perrig, A., Szewczyk, R., Wen, V., Culler, D., Tygar, J. D. *SPINS: Security Protocols for Sensor Networks*. *Wireless Networks*, vol. 8, pp. 521–534, 2002.
- [78] Zhu, S., Setia, S., Jajodia, S. *LEAP plus: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks*. ACM Transactions on Sensor Networks, vol. 2. pp. 500–528, 2006.
- [79] Luk, M., Perrig, A., Whillock, B. *Seven cardinal properties of sensor network broadcast authentication*. In Proceedings of the fourth ACM workshop on security of ad hoc and sensor networks, pp. 147–156, 2006.
- [80] Karlof, C., Sastry, N., Wagner, D. *TinySec: A link layer security architecture for wireless sensor networks*. In Proceedings of the 2nd international conference on embedded networked sensor systems, pp. 162–175, 2004.
- [81] Stouffer, K., Zimmerman, T. Tang, C., Lubell, J., Cichonski, J., McCarthy, J. *Cybersecurity Framework Manufacturing Profile*. National Institute of Standards and Technology, Internal Report 8183, 2017.
- [82] Gül, M. *Intrusion detection for wireless sensor networks using ant colony*. In Signal processing and communication application conference, pp. 1453–1456, IEEE 2016.
- [83] Alaparthy, V. T., & Morgera, S. D. *A multi-level intrusion detection system for wireless sensor networks based on immune theory*. IEEE Access, n° 6, pp. 47364–47373. IEEE 2018.
- [84] Borkar, G. M., Patil, L. H., Dalgade, D., & Hutke, A. *A novel clustering approach and adaptive SVM classifier for intrusion detection in WSN: A data mining concept*. Sustainable Computing: Informatics and Systems, n°. 23, pp. 120–135, 2019.

- [85] Amouri, A., Morgera, S., Bencherif, M., & Manthena, R. *A cross-layer, anomaly-based IDS for WSN and MANET*. *Sensors*, vol. 18, 651, 2018.
- [86] Larijani, H., Ahmad, J., & Mtetwa, N. *A heuristic intrusion detection system for internet-of-things (IoT)*. In *Intelligent computing-proceedings of the computing conference*, pp. 86–98, 2019.
- [87] Nikjoo, M., Tehrani, A. S., Kumarawadu, P. *Secure Routing in Sensor Networks*. *Canadian Conference on Electrical and Computer Engineering*, pp. 978–981, IEEE 2007.
- [88] Karlof, C., Wagner, D. *Secure routing in wireless sensor networks: Attacks and countermeasures*. *Proceedings of the 1st IEEE International Workshop on Sensor Network Protocols and Applications*, pp. 113-127, IEEE 2003.
- [89] Heinzelman, W., Chandrakasan, A., Balakrishnan, H. *Energy-Efficient Communication Protocols for Wireless Microsensor Networks*. *Proceedings of the 33rd Hawaaiian International Conference on Systems Science*, 2000.
- [90] Masdari, M., Bazarchi, S. M., Bidaki, M. *Analysis of Secure LEACH-Based Clustering Protocols in Wireless Sensor Networks*. *Journal of Network and Computer Applications*, vol. 36, pp. 1243-1260, 2013.
- [91] Alshowkan, M., K. Elleithy, K., Alhassan, H. *LS-LEACH: A New Secure and Energy Efficient Routing Protocol for Wireless Sensor Networks*. *IEEE/ACM 17th International Symposium on Distributed Simulation and Real Time Applications*, pp. 215–220, IEEE 2013.
- [92] Kumar, S. R., Umamakeswari, A. *SSLEACH: Specification based secure LEACH protocol for Wireless Sensor Networks*. *International Conference on Wireless Communications, Signal Processing and Networking*, pp. 1672-1676, 2016.
- [93] Selvi, M., Thangaramya, K., Ganapathy, S., Kulothungan, K., Nehemiah, H. K., & Kannan, A. *An energy aware trust based secure routing algorithm for effective communication in wireless sensor networks*. *Wireless Personal Communications*, vol. 105, pp. 1475–1490, 2019.
- [94] Akter, S., Rahman, M. S. Mansoor, N. *An Efficient Routing Protocol for Secured Communication in Cognitive Radio Sensor Networks*. *IEEE Region 10 Symposium*, pp. 1713–1716, IEEE 2020.
- [95] Sokullu, R., Korkmazy, I., Dagdeviren, O., Mitsevax, A., Prasad, N.R. *An investigation on IEEE 802.15.4 MAC layer attacks*. In *Proc. of 10th International Symposium on Wireless Personal Multimedia Communications*, 2007.

- [96] Lichtman, M., Poston, J.D., Amuru, S., Shahriar, C., Clancy, T.C., Buehrer, R.M., Reed, J.H. *A Communications Jamming Taxonomy*. IEEE Security & Privacy, vol. 14, pp. 47–54, 2016.
- [97] Xu, W., Ma, K., Trappe, W., Zhang, Y. *Jamming Sensor Networks: Attack and Defense Strategies*. IEEE Network, vol. 20, pp. 41–47, 2006.
- [98] Strasser, M., Danev, B., Čapkun, S. *Detection of reactive jamming in sensor networks*. ACM Transactions on Sensor Networks, article n°. 16, ACM 2010.
- [99] Yu, M., Su, W., Kosinski, J., Zhou, M. *A new approach to detect radio jammings in wireless networks*. IEEE International Conference on Networking, Sensing and Control, pp. 721–726 IEEE, 2010.
- [100] <https://www.who.int/topics/epidemiology/en/>
- [101] World Health Organization. *Reference Guide on the Content Model of the ICD 11 alpha*. Geneva 2011.
- [102] https://www.who.int/topics/infectious_diseases/en/
- [103] Kermack, W., McKendrick, A. *Contributions to the mathematical theory of epidemics, part I*. Royal Society, vol. 115, pp. 700–721, 1927.
- [104] Brauer, F., Castillo-Chavez, C. *Mathematical Models in Population Biology and Epidemiology*, 2nd edition. Springer 2010.
- [105] Chowell, G., Nishiura, H., Bettencourt, L. M. A. *Comparative estimation of the reproduction number for pandemic influenza from daily case notification data*. Journal of The Royal Society, Interface vol. 4, pp. 155–166. The Royal Society 2006.
- [106] Longini, I. M., Halloran, M. E., Nizam, A., Yang, Y. *Containing pandemic influenza with antiviral agents*. Am. Journ. of Epidemiology, vol. 159, pp. 623–33. 2004.
- [107] Anderson, R.M., May, R.M. *Infectious Diseases of Humans*. Oxford University Press, 1991.
- [108] Gumel, A.B., Ruan, S., Day, T., Watmough, J. et al. *Modelling strategies for controlling SARS outbreaks*. The Royal Society, vol. 271, pp. 2223–2232, The Royal Society 2004.
- [109] White, L.F., Wallinga, J., Finelli, L., et al. *Estimation of the reproductive number and the serial interval in early phase of the 2009 influenza A/H1N1 pandemic in the USA*. Influenza and Other Respiratory Viruses, vol. 3, issue 6, pp. 267–276. 2009.
- [110] Althaus, C.L. *Estimating the Reproduction Number of Ebola Virus (EBOV) During the 2014 Outbreak in West Africa*. PLoS 2014.

- [111] Gao, D., Lou, Y., He, D. et al. *Prevention and Control of Zika as a Mosquito-Borne and Sexually Transmitted Disease: A Mathematical Modeling Analysis*. Sci Rep 6. 2016.
- [112] Zhao, S., Lin, Q., Ran, J., Musa, S., et al. Preliminary estimation of the basic reproduction number of novel coronavirus (2019-nCoV) in China, from 2019 to 2020: A data-driven analysis in the early phase of the outbreak. *International Journal of Infectious Diseases*, vol. 92, pp. 214–217. ScienceDirect 2020.
- [113] Hyafil, A., Moriña, D. *Analysis of the impact of lockdown on the reproduction number of the SARS-Cov-2 in Spain*. *Gaceta Sanitaria*, vol. 35, issue 5, pp. 453–458. Elsevier 2021.
- [114] Diekmann, O., Heesterbeek, J. A. P. and Metz, J. A. J. *On the definition and the computation of the basic reproduction ratio R_0 in models for infectious diseases in heterogeneous populations*. *Journal of Mathematical Biology* N° 28, pp. 365–382, Springer–Verlag 1990.
- [115] Van Den Driessche, P. and Watmough, J. *Reproduction numbers and sub-threshold endemic equilibria for compartmental models of disease transmission*. *Mathematical Biosciences*, N° 180, pp. 29–48, Elsevier 2002.
- [116] Dietz, K. *The estimation of the basic reproduction number for infectious diseases*. *Statistical Methods in Medical Research*, vol. 2, issue 1, pp. 23–41. 1993.
- [117] Heesterbeek, J. A. *A brief history of R_0 and a recipe for its calculation*. *Acta Biotheoretica* vol. 50, pp. 189–204. Kluwer 2002.
- [118] Chowell, G., Tariq, A., Hyman, J.M., *A novel sub-epidemic modeling framework for short-term forecasting epidemic waves*. *BMC Medicine* 2019.
- [119] Ma, J. *Estimating epidemic exponential growth rate and basic reproduction number*. *Infectious Disease Modelling* vol. 5 pp. 129–141. Elsevier 2020.
- [120] Holland, J. *Notes on R_0* . Department of Anthropological Sciences, Stanford University, 2007.
- [121] Brauer, F., Van Den Driessche, P., Wu, J. *Mathematical Epidemiology*. Springer 2008.
- [122] Hethcote, H. *The Mathematics of Infectious Diseases*. *SIAM Review*, vol. 42, pp. 599–653. 2000.
- [123] Barlow, N. S., & Weinstein, S. J. *Accurate closed-form solution of the SIR epidemic model*. *Physica D. Nonlinear phenomena*, vol. 408. 2020.

- [124] Harko, T., Lobo, F.S., Mak, M. *Exact Analytical Solutions of the Susceptible-Infected-Recovered (SIR) Epidemic Model and of the SIR Model with Equal Death and Birth Rates*. Applied Mathematics and Computation, vol. 236, pp. 184–194, 2014.
- [125] Perko, L. *Differential Equations and Dynamical Systems*. 3rd Ed. Springer 2010.
- [126] Blackwood, J.C., Childs, L.M. *An introduction to compartmental modeling for the budding infectious disease modeler*. Letters in Biomathematics, vol. 5, issue 1, pp. 195–221, 2018.
- [127] Turner, M.E. Jr., Bradley, E.L. Jr., Kirk, K.A., Pruitt, K. M. *A theory of growth*. Mathematical Biosciences, Vol. 29, Issues 3–4, PP. 367–373. Elsevier 1976.
- [128] Tolle, J. *Can growth be faster than exponential, and just how slow is the logarithm?* Mathematics Gazete, n°87 pp. 522–525, 2003.
- [129] Savageau, M.A. *Growth equations: A general equation and a survey of special cases*. Mathematical Biosciences, vol. 48, Issues 3–4, pp. 267–278, 1980.
- [130] Chowell, G., Viboud, C., Hyman, J.M., Simonsen, L. *The Western Africa Ebola virus disease epidemic exhibits both global exponential and local polynomial growth rates*. PLoS Curr., n°7, 2015.
- [131] Viboud, C., Simonsen, L. & Chowell, G. *A generalized-growth model to characterize the early ascending phase of infectious disease outbreaks*. Epidemics, n° 15, pp. 27–37. Elsevier 2016.
- [132] Roosa, K., Lee, Y., Luo, R., Kirpich, A., Rothenberg, R., Hyman, J.M., Yan, P., Chowell, G. *Real-time forecasts of the COVID-19 epidemic in China from February 5th to February 24th, 2020*. Infectious Disease Modelling, n°5, pp. 256–263, KeAi 2020.
- [133] Shim, E., Tariq, A., Choi, W., Lee, Y., Chowell, G. *Transmission potential and severity of COVID-19 in South Korea*. International Journal of Infectious Diseases, n° 93, pp. 339–344. Elsevier 2020.
- [134] Del Valle-Soto, C., Mex-Perera, C., Monroy, R., Nolasco-Flores, J. *MPH-M, AODV-M and DSR-M Performance. Evaluation under Jamming Attacks*. Sensors 17, N°. 7, pp. 1–26, 2017.
- [135] Obaid, H. S. *Wireless Network Behaviour during Jamming Attacks: Simulation using OPNET*. Journal of Physics: Conference Series, IOP Publishing, 2020.
- [136] Del Valle-Soto C., Mex-Perera C., Olmedo O., Orozco-Lugo A., Galván-Tejada G., Lara M. *On the MAC/Network/Energy Performance Evaluation of Wireless Sensor*

- Networks: Contrasting MPH, AODV, DSR and ZTR Routing Protocols*. Sensors 2014, N° 14, pp. 22811–22847
- [137] Del-Valle-Soto, C., Lezama, F., Rodriguez, J, Mex-Perera, C., de Cote, E.M. *CML-WSN: A Configurable Multi-layer Wireless Sensor Network Simulator*. In Applications for Future Internet; Springer International Publishing, pp. 91–102, 2017.
- [138] <https://www.ti.com/product/CC2530>
- [139] Meyers, L. A., Pourbohloul, B., Newman, M.E.J., Skowronski, D. M., Brunham, R. C. *Network theory and SARS: predicting outbreak diversity*.
- [140] Lloyd, A. L. and Valeika, S. *Network Models In Epidemiology: An Overview*. Lecture Notes in Complex Systems, Complex Population Dynamics, pp. 189-214, World Scientific, 2007.
- [141] Keeling, M. J. and Eames, K.T. *Networks and epidemic models*. Journal of Royal Society Interface, Vol. 2, pp. 295–307, 2005.
- [142] Rappaport, T.S. *Wireless Communications, Principles and Practice*. 2nd. ed. Prentice Hall, 2002.
- [143] Newman, M. E. J. *The Structure and Function of Complex Networks*.
- [144] World Health Organization, Global Health Observatory (GHO) data https://www.who.int/gho/epidemic_diseases/cholera/case_fatality_rate_text/en/.
- [145] <https://www.mathworks.com/help/optim/ug/lsqcurvefit.html>
- [146] <https://www.mathworks.com/help/optim/ug/least-squares-model-fitting-algorithms.html>
- [147] Gavin, H.P. *The Levenberg-Marquardt algorithm for nonlinear least squares curve-fitting problems*. Department of Civil and Environmental Engineering. Duke University 2020.
- [148] Chowell G. *Fitting dynamic models to epidemic outbreaks with quantified uncertainty: A primer for parameter uncertainty, identifiability, and forecasts*. Infectious Disease Modelling n° 2, pp. 379–398. ScienceDirect 2017.
- [149] Smirnova, A., Chowell, G. *A primer on stable parameter estimation and forecasting in epidemiology by a problem-oriented regularized least squares algorithm*. Infectious Disease Modelling, N° 2, pp. 268–275. ScienceDirect 2017.
- [150] Efron, B., Tibshirani, RJ. *An introduction to the bootstrap*. CRC Press 1994.
- [151] <https://github.com/mjlaine/mcmcstat/blob/master/plims.m>
- [152] Haario, H., Laine, M, Mira A, Saksman E. *DRAM: Efficient adaptive MCMC*. Statistics and Computing N° 16, pp. 339–354, 2009.

- [153] Biggerstaff, M., Cauchemez, S., Reed, C., Gambhir, M., Finelli, L. *Estimates of the reproduction number for seasonal, pandemic, and zoonotic influenza: asystematic review of the literature*. BMC Infectious Diseases, vol. 14. BMC 2014.
- [154] Nishiura, H., Wilson, N., Baker, M. G. *Estimating the reproduction number of the novel influenza A virus (H1N1) in a Southern Hemisphere setting: preliminary estimate in New Zealand*. The New Zealand medical journal vol. 122, pp. 73–77. 2009.
- [155] Ferguson, N., Cummings, D., Fraser, C. et al. *Strategies for mitigating an influenza pandemic*. Nature vol. 442, pp. 448–452. Nature 2006.