MÁSTER EN TECNOLOGÍAS Y APLICACIONES EN INGENIERÍA INFORMÁTICA

TRABAJO FIN DE MÁSTER

UNIVERSIDAD DE ALMERÍA

ESCUELA SUPERIOR DE INGENIERÍA

Líneas de defensa y seguridad en redes ad hoc: un estudio sistemático

Curso 2019/2020

Alumno/a:
Juan Antonio Rodríguez Baeza

Director/es:
Roberto Magán Carrión
Leocadio González Casado

Dedicado a mi padre.

De noche le oigo rezar
esperando que venga volando Peter pan
y le lleve con ella donde nunca jamás
se sentirá como un niño perdido

No sé si oirás mi canción
Pero antes de borrarme de tu imaginación
Te grabo este te quiero al lado de un corazón
Tan bueno como vacío

Agradecimientos

El Padrino parte II.

Retomando mi biografía inacabada desde el TFG, hoy comienzo a escribir lo que debió ser una carta entregada en mano y no pudo ser.

Aunque la primera parte de esta misiva reflejaba un recorrido, como bien decía, precario, las cosas han cambiado para bien en lo que a trabajo se refiere, tampoco podía cambiar mucho a peor. Bueno, pues como decíamos ayer, con la idea de tener la cabeza ocupada durante los lúgubres inviernos en mi Ayamonte odiada y amada... bachiller, FP, Grado... vámonos con el Máster, será por ocupar cabeza, si tengo *pa* donar.

Cambiamos de provincia, nos vamos a Cádiz. Sin terminar el Máster que nos ocupa, se me presenta otra oportunidad de las de agarra y no sueltes. Un Doctorado en Cádiz. Y ya hablaba de titánicos proyectos durante la carrera. Inma coge el petate que nos vamos a Cádiz. El planteamiento de este TFM así como la escritura de esta memoria nacen en la propia necesidad de realizar una contundente revisión de la Literatura y un meticuloso estudio del estado intelectual de una disciplina concreta como comienzo de una Tesis Doctoral. ¿Te has *quedao* sin aire? Como me quedé yo con este tren.

De nuevo tengo que hacer un reconocimiento póstumo. Trabajador inagotable, personaje entrañable, marido incondicional, padre entregado. El otro pilar fundamental en mi vida, al menos esta vez sí me acompaño durante todo el recorrido en tierras de levante. No llegué a comprender si lograbas descifrar aquellos galimatías que te explicaba cuando llegaba de clases contándote lo que había hecho ese día, pero tu interés fue una motivación extra en mis andanzas. A su memoria quiero dedicar la consecución de este TFM con no menos sorpresa, pero con la misma emoción que al anterior trabajo. Espero y deseo que de verdad exista un cielo y lo hayan puesto a vuestro nombre, no he sido un hijo fácil de llevar. Hasta luego padre, dale un beso a madre.

Quien sigue ahí al pie del cañón es mi amada e idolatrada[1] ya esposa, Inma. En serio, a esta tía ahí que hacerla santa. De nuevo asistiome en el peor momento de mi vida, de nuevo apoyo, de nuevo empujón emocional, de nuevo sin capacidad física ni psicológica para agradecerte todo lo que has hecho, y esta vez se une mi padre a este agradecimiento.

Siempre se ha dicho que detrás de una gran mujer viene la suegra. Inma vino con un pack bastante completito, Luis, Antonia, Luis Jr., Toñi, Loli, Michel, Julia y Darío, familia. Yo no tengo palabras para agradeceros que me hayáis acogido de la forma que lo habéis hecho. Cuidasteis de mi padre cuando él más lo necesitó, os doy las gracias en su memoria.

Se acababa la prórroga del partido, muchos se quedaron atrás con calambres y tirones. Algunos valientes siguieron, el ascenso a Segunda B podía materializarse. Urdiales, Mateo, Toni, Llopis, Bordes, Zapata, José Carlos, Manolo. Sin vosotros tampoco se hubiera escrito este trabajo. Chavales, sois grandes.

[1] Según la RAE. Idolatrar. 2. tr. Amar o admirar con exaltación a alguien o algo.

También tengo que acordarme de comandantes. Antonio Corral, Antonio Becerra, Manolo Torres, José Antonio Bermejo, Juan F^{co} Sanjuán, Joaquín Cañadas, Javier Criado, José Antonio Piedra, Pilar, Leo mi director de TFM. De nuevo muchas gracias por vuestra paciencia y dedicación a vuestro trabajo.

En Cadíz también encontré buena gente, como ya he comentado, este trabajo forma parte de un proyecto mucho mayor. Muchas gracias Roberto, también director de este trabajo, por esta gigantesca oportunidad, espero estar a la altura y no defraudar. Igualmente gracias a Patricia, también presente durante la realización de este trabajo. Buenos profesionales de los que aprender mucho.

Además, quiero nombrar a los nuevos compañeros de la UCA. Dani, Leo, Pablo, Kevin, David. Las mañanas en la Escuela se pasan de lujo chavales.

Índice general

Índice de figuras

Índice de tablas

Glosario

Ad hoc Una red ad hoc inalámbrica es un tipo de red inalámbrica descentralizada. 27, 28, 30, 31, 34, 35, 37, 38, 57, 62–64, 67, 70, 73, 75, 78, 80, 81, 89, 93, 94, 97, 101–103, 113

Análisis de Rendimiento El análisis de rendimiento, basado en el resultado de la publicación y las citas recibidas, se utiliza para evaluar el desempeño de la investigación de países, universidades, departamentos o personas. 37, 38, 59

Artificial immune system En inteligencia artificial, los sistemas inmunitarios artificiales son una clase de máquinas de aprendizaje basado en reglas computacionalmente inteligentes, inspiradas en los principios y procesos del sistema inmunitario vertebral. 23, 77

Backend En diseño web hace referencia a la visualización del usuario navegante por un lado (front end), y del administrador del sitio con sus respectivos sistemas por el otro (back end). Muchos métodos conocidos para interactuar con ordenadores pueden ser conceptualizados en términos de front end y back end. 48

Blackhole En un ataque de agujero negro, un nodo malicioso usa su protocolo de enrutamiento para publicitarse por tener la ruta más corta al nodo de destino, descartando todos los paquetes recibidos. 76–78, 92, 93, 95–98, 113

Dataset Un conjunto de datos (conocido también por el anglicismo dataset, comúnmente utilizado en algunos países hispanohablantes) es una colección de datos habitualmente tabulada. 39–42, 59, 60

Delay Retardo de red, también retraso de red, en ciencias de la computación, es un parámetro importante en el diseño y caracterización de una red de telecomunicaciones. El retardo de red especifica cuánto tiempo tarda un bit de datos para viajar a través de la red desde un nodo origen a uno final. 95, 103

Eavesdropping Un ataque de espionaje, también conocido como ataque de rastreo o espionaje, es un robo de información que se transmite a través de una red a través de una computadora, teléfono inteligente u otro dispositivo conectado. El ataque aprovecha las comunicaciones de red no seguras para acceder a los datos mientras los envía o recibe el usuario. 30, 76

Fabrication En este tipo de ataque, un usuario no autorizado inserta un mensaje falso en la red como si fuera un usuario válido. Esto resulta en la pérdida de confidencialidad, autenticidad

e integridad del mensaje. 75

Firewalls En informática, un cortafuegos es la parte de un sistema informático o una red informática que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas. Los cortafuegos. pueden ser implementados en hardware o software, o en una combinación de ambos. 89

Flooding Un ataque por inundación es una forma de denegación de servicio en el que un atacante envía una sucesión de paquetes en *broadcast* al sistema/red objetivo en un intento de consumir suficientes recursos para que dicho sistema no responda al tráfico legítimo. 97

Fuzzy Logic La lógica difusa se basa en lo relativo de lo observado como posición diferencial. Este tipo de lógica toma dos valores aleatorios, pero contextualizados y referidos entre sí. 75

Grayhole En un ataque de agujero gris, un nodo malicioso usa su protocolo de enrutamiento para publicitarse por tener la ruta más corta al nodo de destino, descartando algunos de los paquetes recibidos. 77, 93, 98, 113

Impersonation Un ataque de suplantación de identidad es un ataque en el que un adversario asume con éxito la identidad de una de las partes legítimas en un sistema o en un protocolo de comunicaciones. 75

Jamming Los ataques de interferencia son un subconjunto de los ataques de denegación de servicio (DoS) en los que los nodos maliciosos bloquean la comunicación legítima al causar interferencias intencionales en las redes. Para comprender mejor este problema, necesitamos discutir y analizar, en detalle, varias técnicas de interferencia y antiinterferencia en redes inalámbricas. 30, 76

Machine Learning El aprendizaje automático o aprendizaje automatizado o aprendizaje de máquinas es el subcampo de las ciencias de la computación y una rama de la inteligencia artificial, cuyo objetivo es desarrollar técnicas que permitan que las computadoras aprendan. 103

Man-in-The-Middle En criptografía y seguridad informática, un ataque man-in-the-middle (MITM) es un ataque en el que el atacante transmite en secreto y posiblemente altera las comunicaciones entre dos partes que creen que se están comunicando directamente entre sí. 114

Merkle tree Un árbol hash de Merkle o árbol de merkle o árbol hash es una estructura de datos en árbol, binario o no, en el que cada nodo que no es una hoja está etiquetado con el hash de la concatenación de las etiquetas o valores de sus nodos hijo. Son una generalización de las listas hash y las cadenas hash. 94

Modification Los ataques de modificación de datos (MDA) pueden ser maliciosos y causar enormes daños a un sistema. MDA ocurre cuando los atacantes interrumpen, capturan, modifican, roban o eliminan información importante en el sistema a través del acceso a la red o el acceso directo mediante códigos ejecutables. 93

Multi-hop El enrutamiento de múltiples saltos (o enrutamiento multi-hop) es un tipo de comunicación en redes de radio en las que el área de cobertura de la red es mayor que el rango de radio de los nodos individuales. Por lo tanto, para llegar a algún destino, un nodo puede utilizar otros nodos como relés. 27

Multilayer En el contexto de las redes de computadores, el termino *multilayer* hace referencia a soluciones o implementaciones que hacen uso de mas de una capa ya sea del modelo Open System Interconnection (OSI) o del modelo TCP/IP. 77, 93

OpenSource El software de código abierto es el software cuyo código fuente y otros derechos que normalmente son exclusivos para quienes poseen los derechos de autor, son publicados bajo una licencia de código abierto o forman parte del dominio público. 49, 51

Packet Dropping En las redes de computadoras, un atáque *packet drop* o *blackhole* es un tipo de ataque de denegación de servicio en el cual un router que debe retransmitir paquetes, en lugar de ello los descarta. 19, 30, 31, 63, 64, 68, 73, 78, 94, 95, 98, 113

SPAM Los términos correo basura, correo no solicitado y mensaje basura hacen referencia a los mensajes no solicitados, no deseados o con remitente no conocido, habitualmente de tipo publicitario, generalmente son enviados en grandes cantidades que perjudican de alguna o varias maneras al receptor. 114

SciMAT es una herramienta de software de código abierto (GPLv3) desarrollada para realizar un análisis de mapeo científico bajo un marco longitudinal. SciMAT proporciona diferentes módulos que ayudan al analista a realizar los pasos del flujo de trabajo del mapeo científico. 35, 37, 39, 48, 52, 54, 56, 57, 60–62

Science Mapping desarrollo y aplicación de técnicas computacionales a la visualización, análisis y modelado de una amplia gama de actividades científicas y tecnológicas en su conjunto. 30, 31, 33, 35, 37–39, 54

Scrum Es un marco de trabajo para desarrollo ágil de software que se ha expandido a otras industrias. 39

Sinkhole El ataque de sumidero es un tipo de ataque en el que el nodo comprometido intenta atraer tráfico de red anunciando su actualización de enrutamiento falso. Uno de los impactos del ataque de sumidero es que se puede usar para lanzar otros ataques como el ataque de reenvío selectivo, o ataques de *Packet Dropping*. 92, 113, 114

Smartcities La expresión «ciudad inteligente» es la traducción y adaptación del término en idioma inglés «smart city». Es un concepto emergente, y por tanto sus acepciones en español y en otros idiomas, e incluso en el propio idioma inglés, están sujetas a constante revisión. 27

Smartphones El teléfono inteligente (del inglés smartphone) es un tipo de computadora u ordenador de bolsillo con las capacidades de un teléfono móvil/celular (ej.: llamada telefónica, servicio de mensajes cortos, etc.). 28

Spoofing La suplantación de identidad, en términos de seguridad de redes, hace referencia al uso de técnicas a través de las cuales un atacante, generalmente con usos maliciosos o de investigación, se hace pasar por una entidad distinta a través de la falsificación de los datos en una comunicación. 76

Survey En el contexto de la bibliometría, un survey es una encuesta de fuentes académicas (como libros, artículos de revistas y tesis) relacionadas con un tema específico o pregunta de investigación. A menudo se escribe como parte de una tesis, disertación o trabajo de investigación, con el fin de situar su trabajo en relación con el conocimiento existente. 75, 78, 80

Sybil En seguridad informática, un ataque Sybil ocurre cuando un sistema distribuido es corrompido por una misma entidad que controla distintas identidades de dicha red. 70, 92, 93

Tampering El ataque de manipulación de parámetros se basa en la modificación de los parámetros intercambiados entre el cliente y el servidor con el fin de manipular los datos de la aplicación. 75, 76

Throughput La tasa de transferencia efectiva es el volumen de trabajo o de información neto que fluye a través de un sistema, como puede ser una red de computadoras. 102, 103

Trust Computing La computación confiable, también conocida por las siglas TC es un conjunto de tecnologías propuestas por el Trusted Computing Group que deben cumplir el hardware de los sistemas. Su objetivo es proteger computadoras de programas de ataques que no pueden ser protegidos por soluciones puramente software. 70

Wizard Un asistente de software o asistente de configuración es un tipo de interfaz de usuario que presenta al usuario una secuencia de cuadros de diálogo que lo guían a través de una serie de pasos bien definidos. 52, 61

Wormhole El ataque de agujero de gusano es un ataque grave en el que dos atacantes se ubican estratégicamente en la red. Uno de ellos reenvía toda la información al segundo en lugar de seguir con la ruta normal. 95, 96, 98

Áreas Temáticas En el contexto del Science Mapping, un área temática se corresponderá con un subdominio conceptual detectado durante el análisis. 38, 43, 57, 72, 73

Cienciometría La cienciometría es la ciencia que estudia la producción científica con el fin de medir y analizar la misma. 33

Coseno de Salton El coseno de Salton mide el grado de similitud de dos conjuntos. 39, 40, 43

Estudios primarios Un estudio empírico que trabaja en una pregunta de investigación específica. 45

Estudios secundarios Un trabajo que revisa todos los estudios primarios posibles, con el objetivo de integrar/sin-tetizar evidencia relacionada con una pregunta de investigación específica. 45

Genetic Algorithm En la ciencia de la computación y la investigación de operaciones, un algoritmo genético (GA) es una metaheurística inspirada en el proceso de selección natural que pertenece a la clase más amplia de algoritmos evolutivos (EA). Los algoritmos genéticos se utilizan comúnmente para generar soluciones de alta calidad a los problemas de optimización y búsqueda basándose en operadores inspirados biológicamente como mutación, cruce y selección. 24, 99

Literatura La literatura científica de un área de especialidad es el corpus acumulado de los artículos de investigación que han aparecido en las revistas de ese campo y está considerado como el repositorio principal del conocimiento que define el estado de ese campo (Holmes *et al.* [28]. 30, 31, 34, 35, 37, 44–46, 54, 57, 60, 75, 76, 78, 89, 90, 95, 101

Mensaje *HELLO* Un mensaje HELLO es un paquete especial que se envía periódicamente desde un enrutador para establecer y confirmar las relaciones de adyacencia de la red. 93, 114

Meta análisis Una forma de estudio secundario donde la síntesis de investigación se basa en métodos estadísticos cuantitativos. 45

Open System Interconnection El modelo de interconexión de sistemas abiertos, más conocido como modelo OSI, es un modelo de referencia para los protocolos de la red, creado en el año 1980 por la Organización Internacional de Normalización. 18, 24

Relay El concepto de Relay Node se diseñó como repetidores de radio que recibían, amplificaban las señales de la estación base y las difundían con todo su ruido e imperfecciones. 99, 103

Resiliencia Según la RAE. Resiliencia: Capacidad de un material, mecanismo o sistema para recuperar su estado inicial cuando ha cesado la perturbación a la que había estado sometido. 80

TCP/IP El modelo TCP/IP es una descripción de protocolos de red desarrollado por Vinton Cerf y Robert E. Kahn, en la década de 1970. Fue implantado en la red ARPANET, la primera red de área amplia (WAN), desarrollada por encargo de DARPA, una agencia del Departamento de Defensa de los Estados Unidos, y predecesora de Internet; por esta razón, a veces también se le llama modelo DoD o modelo DARPA. 18

Índice de equivalencia Cuando dos palabras no aparecen nunca juntas, su co-ocurrencia es nula, el índice de equivalencia vale cero. En cambio, cuando dos palabras siempre que aparecen lo hacen juntas en los mismos documentos, el índice de equivalencia es la unidad. Este índice es independiente del tamaño de la muestra. 39–41, 62

Índice de Estabilidad El índice de Estabilidad mide la estabilidad entre dos conjuntos a razón de la similitud del númerod e elementos. 43, 72

Índice de Inclusión El índice de inclusión mide el grado de similitud de dos conjuntos, no está sesgado por el número de elementos como el índice de Jaccard o el coseno de Salton. 43, 62

Índice Jaccard El índice de Jaccard o coeficiente de Jaccard mide el grado de similitud entre dos conjuntos, sea cual sea el tipo de elementos. 39, 40, 43, 62

Índice-h El índice h es un sistema propuesto por Jorge Hirsch, de la Universidad de California, para la medición de la calidad profesional de científicos, en función de la cantidad de citas que han recibido sus artículos científicos. 63, 67

Siglas

ABM Anti-Black Hole Mechanism. 95
ACK Acknowledgement. 96
ACO Ant Colony Optimization. 93
AIS *Artificial immune system*. 77
Anomaly-Based IDS Anomaly-Based Intrusion Detection System. 75
AODV Ad hoc On-Demand Distance Vector. 31, 63, 64, 68, 77, 78, 92–98
AOTDV Ad hoc On-demand Trusted-path Distance Vector. 93, 96
APT Advanced Persistent Threat. 76
ARAN AuthenticatedRouting for Ad hoc Networks. 92
ASRP Ad hoc Secure Routing Protocol. 93
BD Base de Datos. 48
BER Bit Error Rate. 97
BPMN Business Process Model and Notation. 49
BT Block Table. 95
CBDCDDPT Cluster Based Datagram Chunk Dropping Detection and Prevention Technique. 95
CEESRA Cluster based Energy Efficient Secure Routing Algorithm. 96
CH Cluster Head. 94–96, 98
CPS Cyber-Physical System. 70
DB4S DB Browser for SQLite. 48
DoS Denial of Service. 30, 76, 96, 97
DPS Detection and Prevention System. 96
DRI Data Routing Information. 94, 95
DSR Dynamic Source Routing. 77
E2E End-to-end. 103
EDRI Extended Data Routing Information. 94
EHF Extremely High Frequency. 68
FANET Flying Ad hoc NETworks. 28

FPR False Positive Rate. 97
GA Genetic Algorithm. 99
GIMP GNU Image Manipulation Program. 50, 51
GPL GNU General Public License. 54
HANET Heterogeneous Ad hoc NETworks. 28
HIDS Host Intrusion Detection System. 90
HMM Hide Markov Model. 94
IDAR Intrusion Detection & Adaptive Response. 96
IDE Integrated Development Environment. 52, 54
IDS Intrusion Detection System. 30, 77, 90, 94, 95
IDSAODV Intrusion Detection System Ad hoc On-Demand Distance Vector. 92
IETF Internet Engineering Task Force. 76
IoT *Internet Of Things*. 27
IoV *Internet of Vehicles*. 28
IPS Intrusion Prevention System. 89
ISI *Institute for Scientific Information*. 34, 56
ITS *Intelligent Transport System*. 28, 76
LAN *Local Area Network*. 27
MANET Mobile Ad hoc NETworks. 28, 30, 31, 64, 68, 75, 77, 78, 92–98, 101, 103
MiTM Man-in-The-Middle. 117
NFJ Null Frequency Jamming. 93
NIDS Network Intrusion Detection System. 90
NSA Negative Selection Algorithm. 78
OLSR *Optimized Link State Routing*. 93, 94
OSI Open System Interconnection. 18
PDF Portable Document Format. 49, 52
PDR Packet Delivery Ratio. 92, 93, 95, 96, 103
PSO *Particle Swarm Optimization*. 30, 98, 102, 103
QoS Quality of Service. 76, 95
R+D Research and development. 73
RA Random Acknowledgments. 94
RIS *Research Information Systems*. 34
RREP Route REPly. 78, 92, 95, 97
RREQ Route REQuest. 78, 95–97
RSA Rivest Shamir Adleman. 64
SAODV Secure Ad hoc On-Demand Distance Vector. 98
SDN Software Defined Networks. 70
Signature-Based IDS Signature-Based Intrusion Detection System. 75
SLR Systematic Literature Review. 44, 45, 57
SN Suspicius Node. 95
SNR Signal to Noise Ratio. 97
SRD-AODV Secure Route Discovery for the AODV protocol. 97
SRP Secure Routing Protocol. 93
TA Total Acknowledgment. 94
TCP Transmission Control Protocol. 97
TTL Time To Live. 93
UDP User Datagram Protocol. 97
UML Unified Modeling Language. 49

UMSA *User-Controllable MultiLayer Secure Algorithm*. 93
V2I *Vehicle to infrastructure*. 73
V2V *Vehicle to vehicle*. 73
V2X *Vehicle to Everything*. 28, 73
VANET Vehicular Ad hoc NETworks. 28, 30, 31, 75–77, 94, 101, 103
VoIP Voice over IP. 54
VPN Virtual Private Network. 56
WAN *Wide Area Networks*. 27
WANET Wireless Ad hoc NETworks. 92
WoK Web of Knowledge. 56
WoS *Web of Science*. 34, 35, 39, 56–59, 83, 88
WSN *Wireless Sensor Network*. 28, 99
XUL XML User Interface Language. 49

1. Introducción

1.1 Motivación y contexto del trabajo

El avance de la tecnología ha permitido la miniaturización de los elementos necesarios involucrados en la comunicación entre dispositivos. El máximo exponente se tiene en el paradigma *Internet Of Things* (IoT) en donde cientos de miles o incluso millones de dispositivos están conectados entre sí para diferentes objetivos. Un escenario de uso son las *Smartcities*, donde despliegues de dispositivos IoT se utilizan para la monitorización de la polución, mejorar la eficiencia energética, etc. En la Figura 1.1 se muestra un ejemplo conceptual de una *Smartcities*.

Ahora bien, ¿de qué manera se interconectan estos dispositivos? Como no podría ser de otra forma a través de redes de comunicaciones que varían, entre otros aspectos, en su ámbito de actuación como son las *Wide Area Networks* (WAN) o las *Local Area Network* (LAN). Dichas redes pueden tener una infraestructura definida o no en donde existen diferentes dispositivos específicos encargados de controlar, supervisar y facilitar el intercambio de información entre los usuarios o nodos finales de la red. Este es el caso de las redes LAN, por ejemplo, en donde es común la existencia de un dispositivo enrutador encargado de encaminar información entre los propios dispositivos que conforman la red así como su comunicación con otras redes e Internet. Sin embargo, en ocasiones es necesario prescindir de dichos dispositivos debido a las necesidades a cubrir por el propio despliegue de red. Como ejemplo, podríamos pensar en un escenario bélico o después de un desastre natural en donde no existe infraestructura alguna de red y son necesarios otros mecanismos de comunicación entre dispositivos. En estas circunstancias es donde aplican las redes *Ad hoc*[1] [57].

En general, una red *Ad hoc* es una red descentralizada y cuyos dispositivos o nodos se comunican entre sí a través de enrutamiento *Multi-hop* [29] o multisalto. Así, cada uno de

[1] Segun la RAE. Ad hoc: Loc. lat.; literalmente 'para esto'.

Figura 1.1: Servicios y applications IoT en *smartcities*.

los dispositivos puede actuar como nodo final o enrutador. Aunque no es una características necesaria, si que es cierto que es común que una red *Ad hoc* sea inalámbrica por la versatilidad que ofrece. Las redes *Ad hoc* son muy flexibles y con un despliegue rápido, sin una topología fija que ubique los nodos físicamente de forma concreta según objetivos o necesidades. La conectividad de estas redes depende de la cooperación misma de los nodos que hacen uso de la red, por lo que dichos nodos implementan protocolos de enrutamiento desarrollados para tal efecto. La capacidad de comunicación inalámbrica aporta escalabilidad, flexibilidad, versatilidad, despliegue sencillo, y demás características a este tipo de redes.

En la Figura 1.2 se puede observar un esquema de lo que sería una red basada en punto de acceso (Subfigura 1.2(a)) y una red *Ad hoc* (Subfigura 1.2(b)) en la que todos los nodos realizan la función de enrutador.

Algunos ejemplos de redes *Ad hoc* son las *Wireless Sensor Network* (WSN) y redes Mobile Ad hoc NETworks (MANET). Los dispositivos o nodos que conforman estas últimas también pueden ser muy dispares, desde *Smartphones* hasta vehículos (Vehicular Ad hoc NETworks (VANET)) o incluso drones (Flying Ad hoc NETworks (FANET)), es por eso que se habla de un término de mayor inclusión que englobaría a todas estas, Heterogeneous Ad hoc NETworks (HANET) [27]). En la Figura 1.3 se puede ver un esquema, con una cierta generalidad, las redes MANET contienen a las VANET, y estas a su vez a las FANET. [16].

Un caso concreto es el uso de estas tecnologías en lo que ha venido a llamarse el *Internet of Vehicles* (IoV). El futuro Sistema de Transporte Inteligente (*Intelligent Transport System* (ITS)) depende en gran medida del sistema de comunicación vehículo a todo (*Vehicle to Everything* (V2X)) que constituye una parte integral y fundamental de su arquitectura. El objetivo principal de V2X es mejorar la seguridad vial y mejorar la gestión del tráfico. Las comunicaciones V2X definen el intercambio de información de un vehículo con diferentes componentes del ITS,

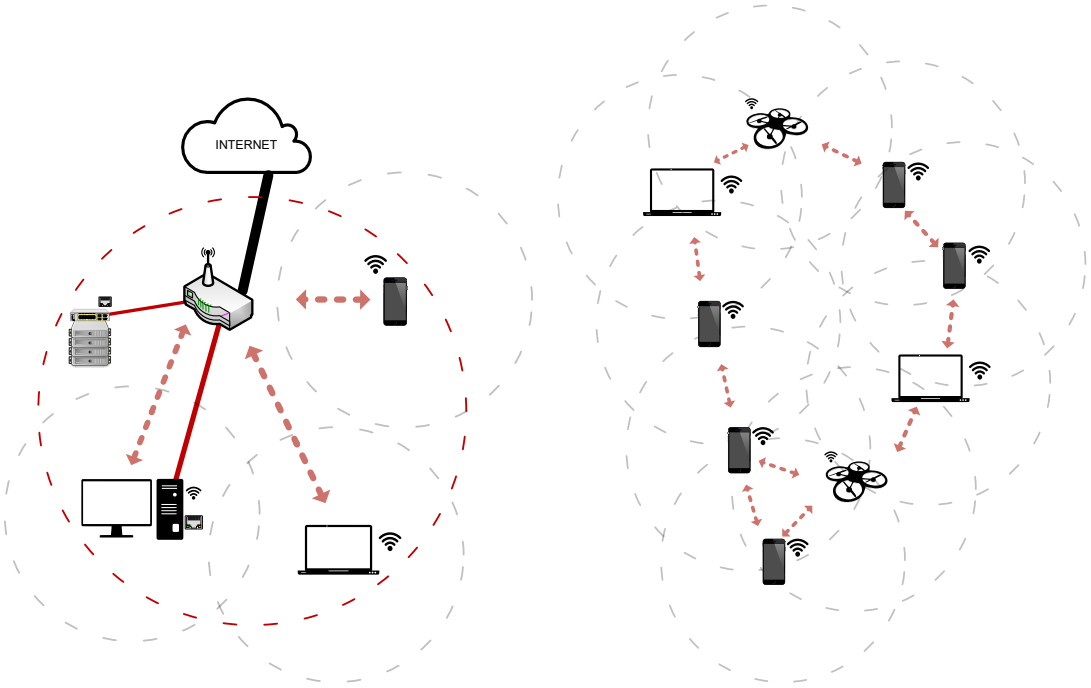


Figura 1.2: Se comparan las topologías de una red basada en punto de acceso en la Subfigura 1.2(a) y una red *Ad hoc* sin punto de acceso en la Subfigura 1.2(b).

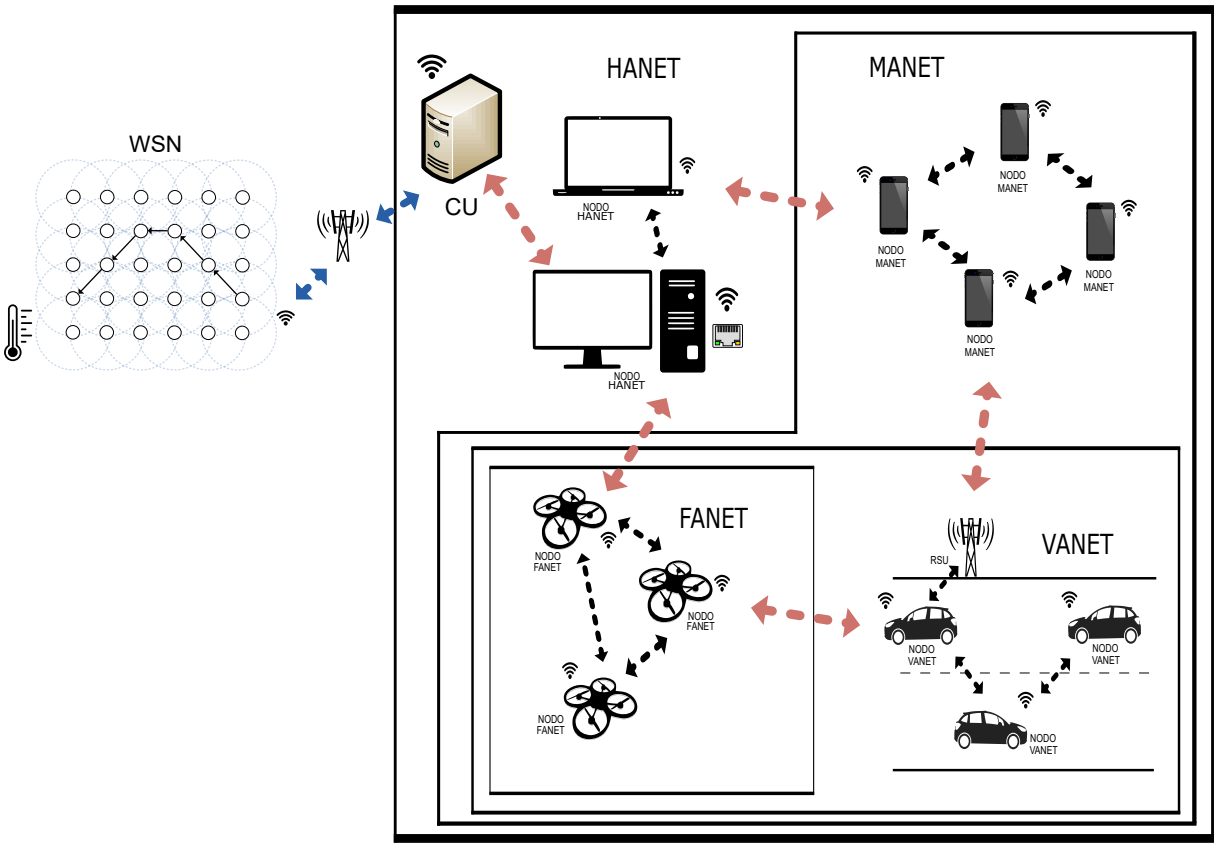


Figura 1.3: Esquema de inclusión de los subconjuntos de redes *Ad hoc*.

incluidos peatones, otros vehículos, infraestructura de transporte (p. ej., señales de tráfico y luces). El uso de las comunicaciones basadas en redes *Ad hoc* estaría justificado en este tipo de entorno, por la necesaria facilidad de conexión y escalabilidad que se debe aplicar al mismo.

Las características de las redes *Ad hoc* las hacen especialmente útiles en situaciones donde, por requisitos del contexto, se precise de un entorno conectado de forma rápida y no tenga el propósito de perdurar en el tiempo, como pueden ser servicios de comunicación militar, eventos de corta duración (deportivos, políticos, ...), gestión de desastres naturales, operaciones de rescate y/o emergencia, etc. Sin embargo, son estas características intrínsecas las mismas que provocan que las redes *Ad hoc* en general y las MANET en particular, sean objeto de multitud de ataques de seguridad en distintas formas, para distintos protocolos y con distintos propósitos.

Los ataques se clasifican según el perjuicio que provocan en la red, así habrá ataques pasivos o activos. Los primeros tratan de escuchar las comunicaciones sin ser descubiertos. Los segundos tienen la intención de interferir en el funcionamiento normal de la red provocando desconexiones de alguna manera.

Uno de los ataques más estudiados es el *Packet Dropping*, que consiste en descartar paquetes deliberadamente. Este ataque se puede realizar de diferentes formas. El ataque por descarte o borrado de paquetes es un tipo de ataque de denegación de servicio (Denial of Service (DoS)) que, como indica su nombre, descarta deliberadamente paquetes de información, para que el origen y el destino perciban la desconexión o degradación de la calidad de la ruta [25]. Otras tipologías de ataque son los *Jamming* que provocan denegación de servicios por interferencias o los de *Eavesdropping* que tratan de interceptar información de manera no autorizada, y una larga lista que clasifican Magán-Carrión *et. al* [42]. En el Anexo A.1, se detallan mejor algunos de estos ataques.

Por todo lo anterior, la comunidad investigadora ha tratado de dar solución a los principales retos planteados en este tipo de redes en relación a su protección frente a amenazas a su seguridad. Por ejemplo, los aspectos fundamentales que debería contemplar una solución de seguridad en dichas redes se comentan en el trabajo de Korde *et al.* [37]. Pero también se realizan estudios que ponen de manifiesto las distintas vulnerabilidades que se puedan encontrar. Por ejemplo, en el trabajo [6], se aborda la problemática asociada a la denegación de servicio en redes VANET. Por otro lado, también se han usado técnicas criptográficas [48], basadas en confianza [40], bio-inspiradas [45] (entre los que destaca el algoritmo *Particle Swarm Optimization* (PSO) [18]), basadas en *clusters* de nodos [82], [31], [63] y [47], al igual que otras muchas técnicas de detección de intrusos (Intrusion Detection System (IDS)) [73], [71], [49], [9] y [80] que tratan de proteger o preservar diferentes servicios de seguridad amenazados por diferentes tipos de ataques.

El presente trabajo intenta recopilar la mayoría de la información acerca del estado del arte en seguridad en redes *Ad hoc* y trata de mostrar al lector la necesidad, primero, de continuar con la investigación en este contexto, y segundo, arrojar luz a la forma de agrupar las distintas soluciones, temáticas asociadas y tendencias que han sido presentadas a lo largo de los años. En este sentido, y como ya se verá a lo largo del trabajo, existe cierta controversia en cómo clasificar dichas soluciones sobre todo en función de la línea de defensa en la que se ubican. Para ello, se ha realizado un estudio pormenorizado a través de un análisis blibliométrico, principalmente con *Science Mapping* [13] y una Revisión Sistemática de la Literatura [36], para obtener la

situación actual de la investigación. Los resultados muestran los claros intentos por solventar la problemática del *Packet Dropping* en lo que respecta al protocolo Ad hoc On-Demand Distance Vector (AODV) [53] y las redes MANET. Además, uno de los objetivos de este trabajo es la categorización de las propuestas de solución existentes. Esto es debido a que las diferentes clasificaciones encontradas no lo hacen de una manera clara, mezclando soluciones en líneas de defensa, o categorizando por algún parámetro menos objetivo. Otro de los resultados que se extraen de este documento, es el creciente interés en la seguridad en redes VANET, quizá derivado de su creciente auge.

1.2 Objetivos

Los principales objetivos del proyecto son:

- Estudio de la evolución, tendencias y temáticas relevantes en redes *Ad hoc*. Para llevar a cabo este objetivo se utilizarán bases de datos científicas, donde se realizarán búsquedas exhaustivas de material y se someterán a análisis de *Science Mapping*. El objetivo es visualizar la evolución de la investigación en lo que concierne a seguridad en redes *Ad hoc*.
- Estudio de soluciones específicas y estado del arte. A partir de las principales tendencias y temáticas anteriores se realizará una búsqueda específica y sistemática de la Literatura haciendo hincapié en las diferentes clasificaciones de soluciones propuestas en la Literatura.
- Propuesta de nuevas taxonomías, retos y líneas investigación. A partir de los trabajos y tareas anteriores se propondrán nuevas taxonomías que ayuden a clasificar e identificar soluciones en líneas de defensa, así como la propuesta de nuevas líneas y retos de investigación no cubiertos en la Literatura.

1.3 Estructura del documento

Este trabajo se estructura en los siguientes capítulos:

- Capítulo 1. Introducción. Se muestran una introducción y motivación de la investigación realizada.
- Capítulo 2. Definición de tareas y planificación. Se presentan y comentan brevemente las fases de realización de este trabajo, acompañado por un cronograma con las horas correspondientes a cada tarea, para justificar el ajuste con la temporización correspondiente al TFM.
- Capítulo 3. Herramientas y métodos. Se presentan las metodologías, herramientas, y en general la forma de llevar a cabo la investigación realizada.
- Capítulo 4. Estudio y análisis de la Literatura. Se estudian los diferentes análisis y mapeados de la investigación realizada en el entorno de la seguridad en redes *Ad hoc*, se plantea la revisión sistemática que se ha llevado a cabo. Esto nos permite tener una panorámica del estado del arte en esta disciplina.
- Capítulo 5. Conclusiones y trabajo futuro. Se muestran las conclusiones y se establece el trabajo futuro.

2. Definición de tareas y planificación

En este capítulo se describen las tareas que se han llevado a cabo a lo largo del proyecto, cuantificando el tiempo dedicado a cada una para ajustar el proyecto al marco para TFMs de la Escuela Superior de Ingeniería de la UAL.

2.1 Definición y descripción de tareas

A continuación se exponen las tareas y subtareas de las que se que compone el proyecto.

2.1.1 Estudio bibliométrico

La bibliometría es el uso de métodos estadísticos para analizar libros, artículos y otras publicaciones [5]. Las técnicas y métodos bibliométricos se utilizan con frecuencia en las bibliotecas y las ciencias de la información. El subcampo de la bibliometría que se ocupa del análisis de publicaciones científicas se llama Cienciometría. El análisis de citas es un método bibliométrico comúnmente utilizado, que se basa en la construcción de gráficos de citas (una red o representación gráfica de las citas entre documentos). Muchos autores utilizan este tipo de técnicas para explorar el impacto de su trabajo o el impacto de un artículo en particular, autor o autores en un determinado campo de investigación.

Por otro lado, el *Science Mapping* se basa en el empleo de herramientas de visualización de datos que ayudan a los científicos a comparar su trabajo y su campo de investigación en relación con las tendencias actuales de investigación y desarrollo. Además, el *Science Mapping* amplía el campo de visión de un científico, le permite comprender la evolución de su investigación, le ayuda a trazar futuros caminos de estudio y le ayuda a expandir sus horizontes de investigación

para abarcar otras disciplinas.

Durante esta fase del proyecto se ha llevado a cabo una búsqueda metodológica en bases de datos científicas digitales como la *Web of Science* (WoS)[1], que permiten exportar la información obtenida en formatos adecuados para el tratamiento estadístico propio de estas técnicas, como por ejemplo el formato *Institute for Scientific Information* (ISI), WoS, o el *Research Information Systems* (RIS). Esa información se ha pasado a herramientas de análisis estadístico y bibliométrico para su posterior interpretación.

2.1.2 Revisión sistemática de la Literatura

Las revisiones sistemáticas de la Literatura utilizan métodos y técnicas sistematizadas para recopilar información, evaluar críticamente los estudios de investigación y analizar los resultados bien de forma cualitativa o cuantitativa. Las revisiones sistemáticas formulan preguntas de investigación de alcance amplio o estrecho, e identifican y sintetizan estudios que se relacionan directamente con la pregunta de revisión sistemática. Están diseñados para proporcionar un resumen completo y exhaustivo de la evidencia actual, publicada y no publicada, siendo metódica, integral, transparente y replicable.

Si bien las revisiones sistemáticas a menudo se aplican en el contexto biomédico o de atención médica, se pueden usar en otras áreas donde sería útil una evaluación de un tema definido con precisión. Las revisiones sistemáticas pueden examinar pruebas clínicas, intervenciones de salud pública, intervenciones ambientales, intervenciones sociales, efectos adversos y evaluaciones económicas. Pero también pueden examinar, en general, el estado de la arte de una disciplina.

Durante esta fase del proyecto, se han realizado nuevas búsquedas metodológicas en diferentes bases de datos (WoS y Scopus, entre otras) en diferentes periodos temporales, y con diferentes terminologías para filtrar la información, con la intención de llevar a cabo una revisión sistemática de la Literatura en lo que concierne a la clasificación de soluciones de seguridad en redes *Ad hoc*.

2.1.3 Propuesta de nuevas taxonomías

Una vez analizada convenientemente la Literatura, en este trabajo se propone una nueva taxonomía que ayude a clasificar las soluciones existentes en el campo de la seguridad en redes ad hoc. Se prestará especial atención a la clasificación por líneas de defensa para la que es posible que se requiera la definición de nuevas líneas que ayuden a la comprensión y estudio de las propuestas actuales.

[1] Web of Science

2.2 Planificación temporal

Seguidamente, se comentan brevemente las tareas realizadas en el proyecto, y se establece la temporización.

1. Estudio bibliométrico: análisis de rendimiento y *Science Mapping*. Utilizando bases de datos científicas se realizarán búsquedas de material con el objetivo de comprender como se ha desarrollado la investigación alrededor del tema o temas que se tratan en este trabajo. 75 horas.
   a) Búsqueda metodológica de información en WoS. 25 horas.
   b) Análisis de la información extraída con la herramienta *SciMAT*. 50 horas.
2. Revisión sistemática de la Literatura. Basada en el uso de metodologías [36] para la búsqueda, filtrado y análisis de trabajos relacionados con la disciplina (seguridad en redes *Ad hoc*). 100 horas.
   a) Identificación de recursos. 20 horas.
   b) Selección de estudios. 20 horas.
   c) Evaluación de la calidad del estudio. 20 horas.
   d) Extracción de datos y seguimiento del progreso. 20 horas.
   e) Síntesis de datos. 20 horas.
3. Propuesta de nuevas taxonomías. A partir de los trabajos y tareas anteriores se propondrán nuevas taxonomías que ayuden a clasificar e identificar soluciones en líneas de defensa, así como la propuesta de nuevas líneas y retos de investigación no cubiertos en la Literatura. 75 horas.
4. Redacción de la memoria para el TFM. 50 horas.

A continuación se exponen la planificación temporal del proyecto, a través de un diagrama de Gantt (Figura 2.1), en donde se muestra de forma visual y cuantitativa la duración estimada para cada una de las tareas definidas anteriormente.

Se ha decidido seguir una metodología tradicional en cascada, ya que las tareas que se necesitan terminar están bien definidas y acotadas en el tiempo, aunque hoy en día están ampliamente extendidas las metodologías ágiles, que son más favorables desde un punto de vista multidisciplinar en un equipo de trabajo.

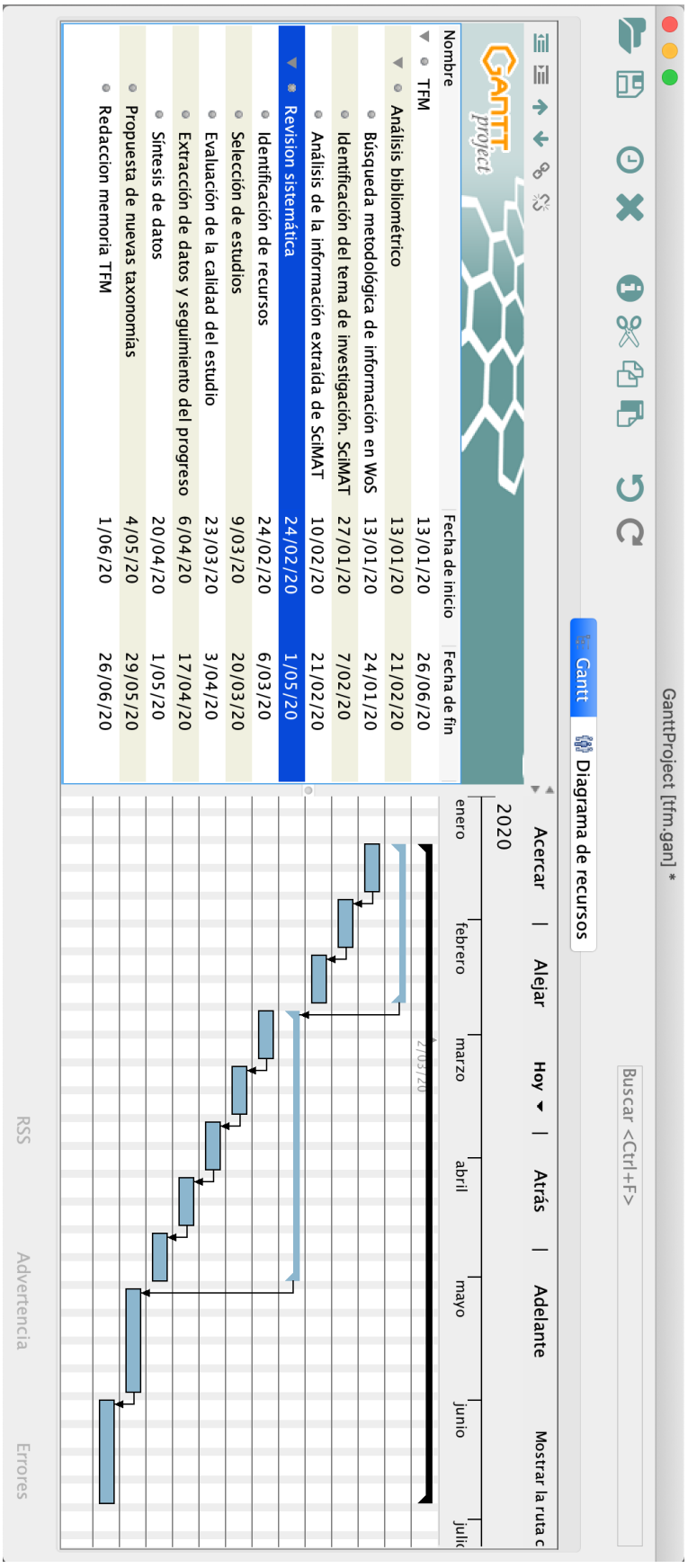


Figura 2.1: Diagrama de Gantt del TFM.

3. Herramientas y métodos

A lo largo del capítulo se presenta y describe la metodología usada durante la realización de este trabajo. La metodología consta de un análisis bibliométrico de la disciplina de investigación *seguridad en redes Ad hoc*, un proceso de *Science Mapping*, y una revisión sistemática de la Literatura en este campo. Concretamente, y enlazando con las fases comentadas en el Capítulo 2, primero se realiza un estudio bibliométrico con el que localizar las temáticas principales y sus conexiones con subtemas de interés, seguidamente se realiza una revisión sistemática de la Literatura.

3.1 Estudio bibliométrico: análisis de rendimiento y *science mapping*

En bibliometría, existen dos procedimientos principales: *Análisis de Rendimiento* y *Science Mapping* [51] [55].

Un *Análisis de Rendimiento* mide, estadísticamente, la información que correlaciona a dos o más documentos bibliográficos, como pueden ser citas o palabras clave, ofreciendo un marco estadístico robusto para llegar a conclusiones. A través de estas metodologías, por ejemplo, se explora el impacto de autores, el número de citas y co-citas que posee un autor o un artículo, se construyen mapas conceptuales, etc. En el caso del presente trabajo, se realiza un breve *Análisis de Rendimiento* para el cómputo de documentos por año en la última década, con la intención de corroborar el dinamismo de la investigación en la disciplina estudiada.

Por otro lado, el *Science Mapping* de una determinada disciplina de investigación, representa gráficamente el estado del arte, pudiendo apreciarse como autores, documentos, temas relevantes y tendencias están interrelacionados. Para este tipo de análisis existen herramientas software, como *SciMAT* [12]. De hecho, el Dr. M.J Cobo hace una revisión del estado del arte en [14], en lo que se refiere a herramientas software para la realización de los mencionados análisis. *SciMAT*

combina el *Science Mapping* y las técnicas de *Análisis de Rendimiento* para estudiar un campo de investigación y visualizar e identificar temas o *Áreas Temáticas* generales y su evolución.

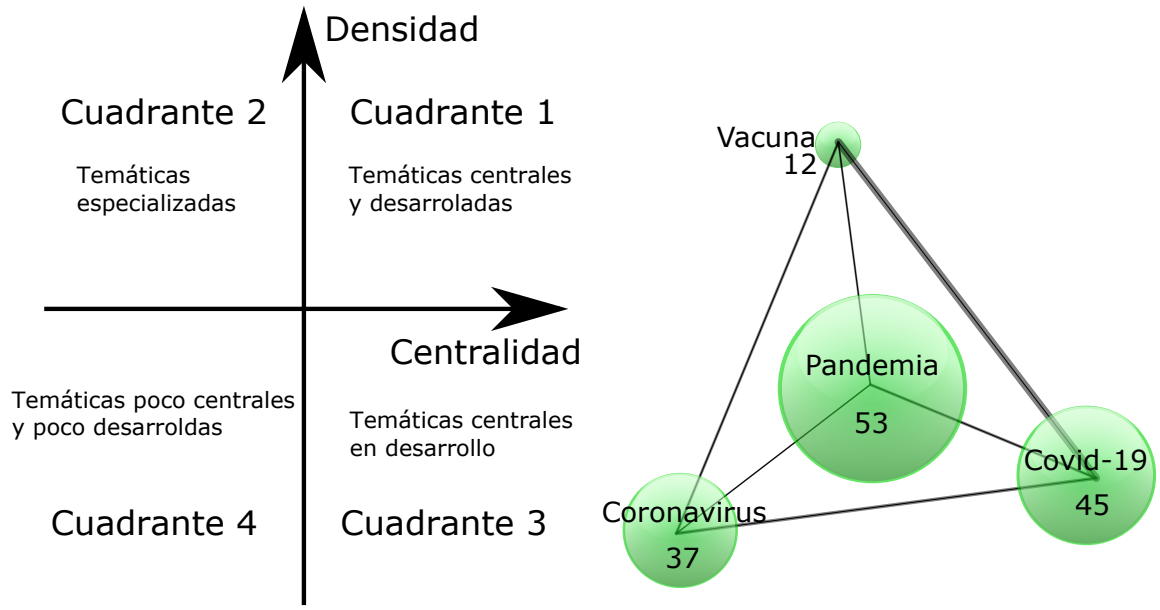
Gracias al estudio bilbliométrico, se conformarán una serie de mapas bibliométricos del campo investigado, para delimitar áreas de investigación. Dos tipos de mapeos son los más utilizados, la citación de documentos y el análisis de co-palabras. El primero sintetiza un área de investigación analizando las citas conjuntas de pares de documentos, mientras que el segundo analiza la información de palabras clave compartidas por conjuntos de documentos. El resultado de cualquiera de estas técnicas devuelve conjuntos agrupados ya sean de referencias (representando la situación intelectual de los diferentes grupos o sub áreas), o de información textual (que representan conjuntos de conceptos/temas que se tratan en el área estudiada). Estas mediciones son capaces de dar resultados de manera longitudinal en el tiempo, pudiendo analizar varios periodos. Por ejemplo, un análisis longitudinal de citaciones muestra la continuidad de la situación intelectual, si el análisis es de co-palabras lo que mostrará será la evolución de los temas de investigación del área tratada.

La visualización de los posibles resultados se realiza a través de diferentes técnicas como son la cadena de clúster [67], [68] y [76], el agrupamiento rodante [77] y los diagramas aluviales [78]. Otra manera de plasmar resultados extraídos de estos análisis es a través de la integración del mapeo y la evaluación del rendimiento, con lo que se podrán cuantificar temas y sub-temas del área de conocimiento estudiada y su evolución, pudiendo medir así el impacto de un campo/sub-campo en un periodo concreto. Para la visualización de estos últimos datos, existen diagramas estratégicos, mapas auto-organizados, mapas heliocéntricos, modelos geométricos y redes temáticas.

En resumen, la co-cita analiza el estado intelectual de un campo de investigación científica y la co-palabra analiza el estado conceptual. El objeto de estudio de este TFM es descubrir la evolución conceptual en el campo de la seguridad en redes *Ad hoc*, por esa razón se hace más adecuado el análisis de co-palabras. Definiendo una lista de palabras clave para el campo de investigación, se puede generar un grafo en el que las palabras sean los vértices y las relaciones entre las palabras sean sus aristas. Así, dos vértices conectados por una arista significarán la existencia de las palabras clave correspondientes en los mismos documentos, si además se asigna peso a esa arista, se puede detectar la importancia de dicha relación en el conjunto global de documentos analizado. Como resultado, se obtendrá una lista de temas/subtemas por periodo estudiado, que, en el caso propuesto, se plasman en un diagrama estratégico conceptual como el mostrado en la Subfigura 3.1(a), acompañado de una serie de grafos correspondiente a cada tema y sub-temas asociados, como el mostrado en la Subfigura 3.1(b). Estas figuras se usan para apoyar la explicación de la Página 41.

De forma esquemática, todo el proceso consta de las siguientes etapas:

1. Adquisición y procesado de datos. Desde bases de datos bibliográficas, se realizan búsquedas que aporten un número considerable de documentos relacionados con la disciplina. Como primer paso, se realiza un *Análisis de Rendimiento* para cuantificar el estado de la investigación. A continuación, se exportan los registros devueltos por la base de datos, los meta-datos correspondientes en formatos adecuados para trabajar con ellos en sistemas de bases de datos locales, con la finalidad de limpiar y adecuar esos datos.
2. Configuración del análisis de co-palabras. Mediante esta etapa se detectan los temas



(a) Diagrama estratégico

(b) Red temática

Figura 3.1: Figuras conceptuales del proceso analítico de co-palabras. En la Subfigura 3.1(a) se ve un diagrama estratégico conceptual, y en la Subfigura 3.1(b) se ve una red temática conceptual. (No se trata de un ejemplo real).

(por período). Usando herramientas software diseñadas para realizar análisis estadísticos bibliométricos, se extraen datos concluyentes del estado del arte en una disciplina en lo que respecta a temáticas, la situación intelectual, evolución de la disciplina, etc. En el caso de este trabajo son temas.

3. Estudio de los resultados. Se enmarcan esos temas en un espacio de baja dimensión, posicionándose de manera estratégica según la importancia relativa de cada tema. Se analiza la evolución temporal de dichos temas detectados a lo largo de los subperíodos.

Todo el proceso es iterativo. En la Figura 3.2 se muestra un diagrama conceptual del proceso, abstraído en un flujo de tipo *Scrum*[1]. Se han hecho revisiones semanales del proceso de depuración, configuración y lectura de los resultados. En esta tarea también han participado el director de este trabajo y personal experto en la disciplina.

Como se ha mencionado anteriormente, el *Science Mapping* muestra de forma gráfica temas y conceptos de un determinado campo de investigación así como sus relaciones y evolución. En el presente trabajo se utiliza *SciMAT* por su relevancia y aceptación dentro de la comunidad investigadora. *SciMAT* es un software escrito en Java por el Dr. M.J. Cobo [13]. Se trata de una aplicación para la cartografía científica que permite realizar estudios basados en el análisis de de co-palabras[8], citas/co-citas [66], referencias de autor, etc. Además, permite el uso de diferentes medidas de normalización o similitud de los datos como pueden ser el Índice de equivalencia o el de inclusión, además del Índice Jaccard o el Coseno de Salton, entre otras opciones.

El proceso de extracción de temas y conceptos pasa por una serie de etapas, empezando por la búsqueda de un *Dataset* que englobe una buena colección de artículos relacionados con el tema de investigación, para lo que se acude a fuentes como la WoS o *Scopus*. En estas bases

[1] El flujo de Scrum

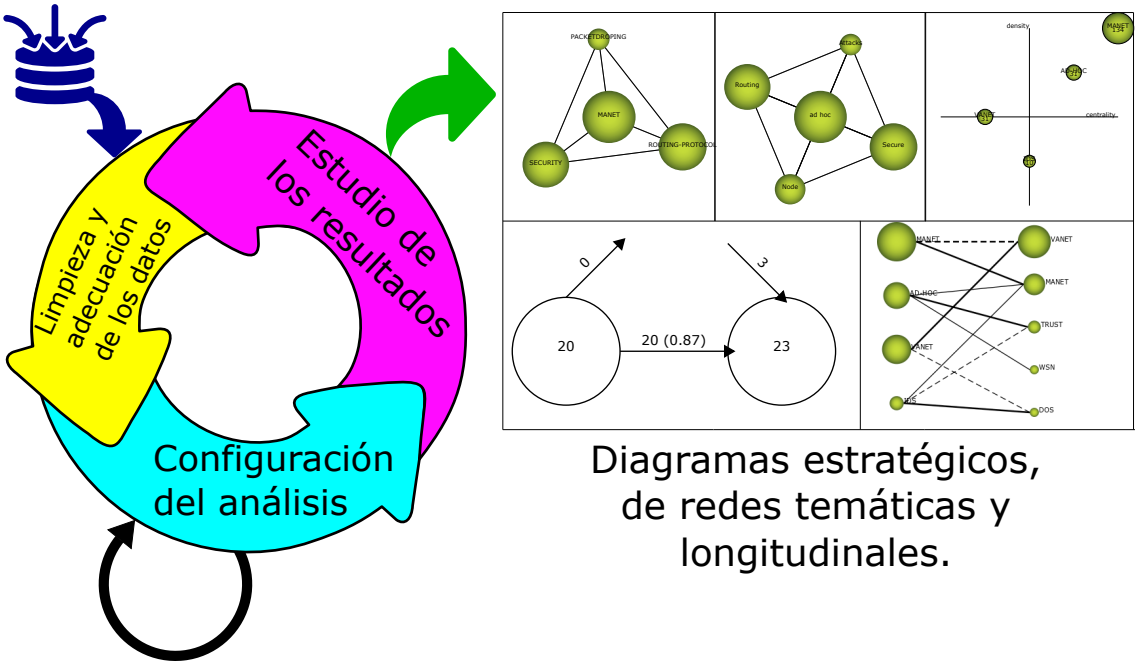


Figura 3.2: Diagrama de flujo iterativo del proceso completo de adquisición, limpieza y procesado de datos, configuración del análisis y estudio de los resultados.

de datos podremos realizar, como decimos, una búsqueda por palabras clave que devuelva un resultado con el mayor número de documentos posible, que después se irá filtrando y definiendo.

A continuación se seleccionan los tipos de elementos a analizar. Estos serán las revistas, los autores, las *keywords*, etc. Por ejemplo, en el caso de este trabajo, se seleccionan las palabras clave, ya que nuestro análisis será de co-palabras. Este incluirá tanto las palabras clave de autor como las indexadas por la fuente. La metodología explicada a continuación se extrae del trabajo de Cobo *et al.* [11].

Seguidamente se extrae la información relevante del *Dataset*. Al ser este un análisis de co-palabras, la información de la que hablamos es la frecuencia de coincidencia de dos palabras, que se define como el número de documentos en los que las palabras aparecen juntas.

Una vez que se tiene una buena cantidad de elementos analizables, se establece un cálculo de similitudes en función de aquellas frecuencias de coincidencia de las palabras clave. Para esta tarea se usan medidas de similitud como el Coseno de Salton y el Índice Jaccard. Según algunos autores [19], la medida más apropiada para normalizar las frecuencias de concurrencia es el Índice de equivalencia (fuerza de asociación, índice de proximidad o índice de afinidad). El Índice de equivalencia $EquivalenceIndex_{ij}$ se define tal como muestra la Ecuación 3.1:

$$EquivalenceIndex_{ij} = \frac{c_{ij}^2}{c_i c_j} \tag{3.1}$$

donde c_{ij} es el número de documentos en los que coexisten dos palabras clave i y j, y c_i y c_j representan el número de documentos en los que aparece cada una. Cuanto más aparezcan juntas el par de palabras, más se acercara a 1 el Índice de equivalencia.

Finalmente, se realiza un agrupamiento de temas/subtemas, con el que se pretenden localizar centros de interés o problemas de investigación fuertemente vinculados, en los que se haya invertido (o se este invirtiendo, depende del período que se este visualizando) un gran carga de trabajo.

En el caso concreto del presente trabajo, se ha usado el Algoritmo de Centros Simples [15]. Se trata de un mecanismo ampliamente usado en el análisis de co-palabras, así como en la construcción de redes temáticas conceptuales, como la que aparece en la Figura 3.1(b). En dicha red se observa como el tema Covid-19 y Vacuna co-ocurren fuertemente (su enlace es grueso), es decir, cada vez que aparecen en un texto analizado van juntas. Además, podemos ver como el tema Pandemia, el que más diámetro tiene, indica que se trata del tema más central de esa red, marcando la posible temática tratada.

Cabe la posibilidad de que dos palabras aparezcan con escasa frecuencia en todo el *Dataset*, pero que siempre lo hagan juntas, lo que implicaría valores de fuerte cohesión en asociaciones posiblemente irrelevantes. El algoritmo es capaz de omitir este contratiempo al permitir configurarlo con frecuencias mínimas y umbrales de co-ocurrencia. De esta forma solo se consideran enlaces potenciales los pares de palabras que excedan dichos parámetros. Además, la posibilidad de limitar el tamaños de las redes a un mínimo y un máximo, permite también acotar el tamaño de los temas detectados.

Si bien las redes temáticas ofrecen una visión de las relaciones entre temas y su co-ocurrencia, los diagramas estratégicos posicionan dichas redes o temas en función de, principalmente, su relevancia dentro del periodo bajo estudio. Las estructuras de red detectadas se representan en dos dimensiones, centralidad y densidad, ambas definidas por Callon *et al* [7], como se aprecia en la Subfigura 3.1(a).

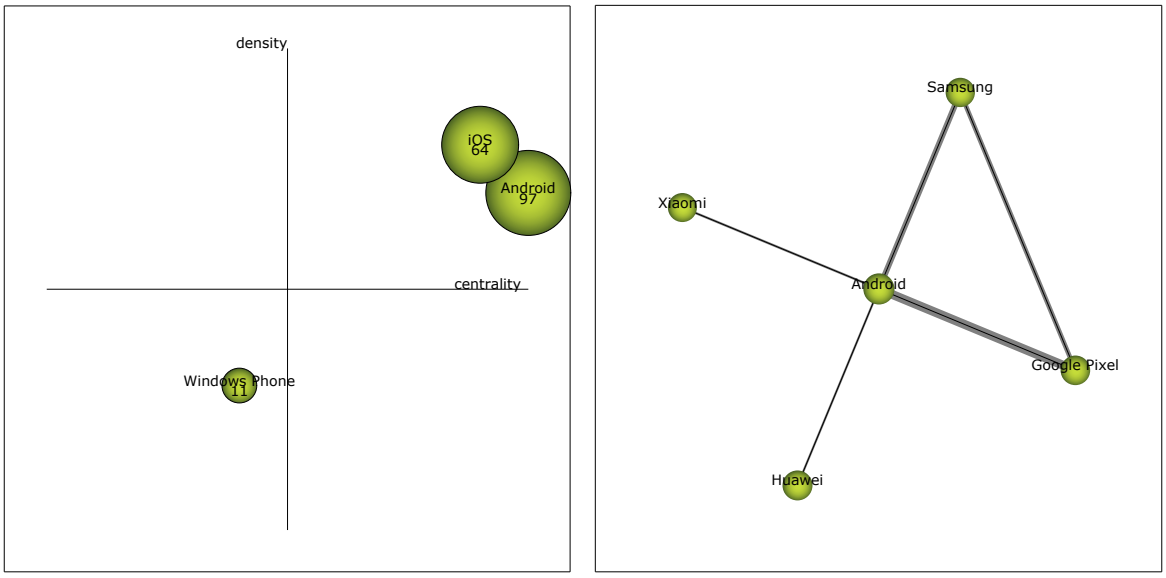
En la Subfigura 3.3(a) vemos un ejemplo de un diagrama estratégico. En dicho diagrama se pueden ver los temas clave detectados. Estos conformaran un cluster cada uno, englobando sus temas asociados y conformando la red temática de cada mencionado tema. Así se genera otro tipo de gráfico llamado red temática, una por cada tema clave descubierto. Cada una de estas redes temáticas se etiqueta con el nombre de la palabra clave más significativa del tema que trate (generalmente será la más central). El volumen de las esferas será proporcional al número de documentos, mientras que el grosor de la arista entre dos esferas i y j será proporcional al Índice de equivalencia. En la Figura 3.3(b) se ve un ejemplo de una red temática.

La centralidad mide el grado de interacciones entre redes o grupos, a lo que el autor llamó enlaces externos. Cuanto más numerosos y fuertes sean estos vínculos, más designará este grupo un conjunto de problemas de investigación considerados cruciales por la comunidad científica o tecnológica. Se define en la siguiente Ecuación 3.2:

$$Centrality = 10(\sum e_{kh}) \tag{3.2}$$

donde k es una palabra clave perteneciente al tema y h una palabra clave que pertenece a otros temas. Esta propiedad mide la fuerza de los enlaces externos, y significará la importancia de un tema en el desarrollo de toda la investigación.

La densidad caracteriza la fuerza de los enlaces que unen las palabras que forman el grupo, a lo que el autor llamó enlaces internos. Cuanto más fuertes son estos vínculos, mejor se constituye



(a) Diagrama estratégico (b) Red temática

Figura 3.3: En la Subfigura 3.3(a) se ve un diagrama estratégico genérico y en la Subfigura 3.3(b) se ve una red temática genérica. (No se trata de un ejemplo real).

un todo coherente e integrado a partir de los problemas de investigación correspondientes al clúster. Se define en la siguiente Ecuación 3.3:

$$Density = 100(\sum \frac{e_{ij}}{w}) \tag{3.3}$$

donde las palabras clave i y j pertenecen al tema, mientras w es el número total de palabras clave en el tema. El valor de la densidad se entiende como una medida de lo desarrollado del tema.

La forma de interpretar un diagrama estratégico y la relevancia del tema en función del cuadrante en donde se localiza es la siguiente:

- **Cuadrante superior derecho**. En este se encuentran temas bien desarrollados y de importancia dentro del campo de investigación estudiado. Son temas motores de la especialidad.
- **Cuadrante superior izquierdo**. Podemos encontrar aquí temas con fuerte cohesión interna, pero débil interconexión externa. Temáticas muy concretas y especializadas.
- **Cuadrante inferior izquierdo**. Temas poco desarrollados tanto interna como externamente. Podría tratarse de temas emergentes en desarrollo que aún no han conectado con otros temas o temas en declive o desaparecidos.
- **Cuadrante inferior derecho**. Temas poco desarrollados y sin embargo con una fuerte interconexión externa. Podrían ser temas o tecnologías transversales o base, consolidadas y ampliamente utilizadas.

Otra opción del estudio es dividir el *Dataset* en períodos conformados por años o grupos de años, o subperíodos temporales consecutivos en general, permitiendo analizar la evolución de los temas del campo de investigación. A este análisis se le llama análisis longitudinal.

Se define T^t como el conjunto de todos los temas del subperíodo t. $U \in T^t$ representa un tema detectado en t y $V \in T^{t+1}$ representa un tema detectado en el siguiente subperíodo $t+1$. Se

dirá que existe una evolución temática del tema U al tema V si se encuentran palabras clave en ambas redes temáticas asociadas. O lo que es lo mismo, U es un tema pasado de V. Las palabras clave k tal que $k \in (U \cap V)$ se consideran nexos temáticos o nexos conceptuales. Los llamados *mapas bibliométricos de evolución* se generan con estos conjuntos de temáticas, vinculados de T^t a T^{t+1} a través de los nexos conceptuales.

Estos nexos son mensurables, ya que se puede cuantificar su importancia ponderando los elementos que comparten para establecer la similitud entre temas con técnicas como el Coseno de Salton o el Índice Jaccard. Sin embargo, estas técnicas son menos aconsejables al estar sesgadas por el número de elementos. Es más recomendable ponderar las palabras clave de cada tema con otra técnica conocida como Índice de Inclusión. El Índice de Inclusión lo definen en el trabajo [11] a través de la siguiente Ecuación 3.4:

$$InclusionIndex = \frac{|(U \cap V)|}{min(|U|,|V|)} \tag{3.4}$$

siendo $|(U \cap V)|$ el valor absoluto del total de elementos compartidos por los conjuntos U y V. Y $min(|U|,|V|)$ el mínimo de los valores absolutos correspondientes a cada conjunto. Siendo k las palabras clave de U tal que $\forall k \in U, k \in V \Rightarrow InclusionIndex = 1$.

Al calcular los índices de inclusión se pueden dar situaciones en las que los temas de diferentes periodos compartan nombre por estar etiquetados con las mismas palabras clave centrales. También pueden darse situaciones en las que los temas compartan palabras clave que no sean el nombre de esos temas. En ambas situaciones se habrán generado *Áreas Temáticas* alrededor de esos temas. Sin embargo, también se pueden dar situaciones en las que un tema no tenga ningún enlace. Se dirá entonces que ese tema se ha suspendido (si es del subperíodo anterior) o que es nuevo (si es del subperíodo posterior).

En la Figura 3.4 se muestra un ejemplo de lo que sería un diagrama de evolución temporal de dos subperiodos consecutivos, P_1 y P_2, con temas detectados en ambos periodos tal que: T_1 es el conjunto de los temas de P_1 y T_2 el conjunto de los temas de P_2, siendo t_n los temas de T_1 y t_m los de T_2. Se observa como se han generado dos *Áreas Temáticas* $A_1 \supset [t_{n1}, t_{m1}]$ y $A_2 \supset [t_{n2}, t_{m2}, t_{m3}]$, mientras que el tema t_{n3} se considerará como suspendido y el tema t_{m4} como nuevo. Las líneas continuas significan que los temas vinculados comparten el nombre: ambos temas tienen el mismo nombre, o el nombre de uno de los temas es parte del otro tema. Una línea de puntos significa que los temas comparten elementos que no son el nombre del tema. El grosor de las líneas es proporcional al Índice de Inclusión, y el volumen de las esferas es proporcional al número de documentos publicados de cada tema.

De una forma similar se podrá medir la estabilidad entre los dos subperiodos consecutivos, para lo que se usa el Índice de Estabilidad de Small, Henry G. [69]. Este índice se define como muestra la Ecuación 3.5:

$$StabilityIndex = \frac{E_{P_1} \bigcap E_{P_2}}{(E_{P_1} \bigcup E_{P_2}) - (E_{P_1} \bigcap E_{P_2})} \tag{3.5}$$

siendo E_{P_1} los elementos del subperiodo anterior y E_{P_2} los del subperiodo posterior, siempre que P_1 y P_2 sean dos subperiodos consecutivos.

El estudio que se realiza es de co-palabras. Por lo tanto, el resultado será el número de palabras clave compartidas por subperiodos consecutivos. En la Figura 3.5 se observa un ejemplo

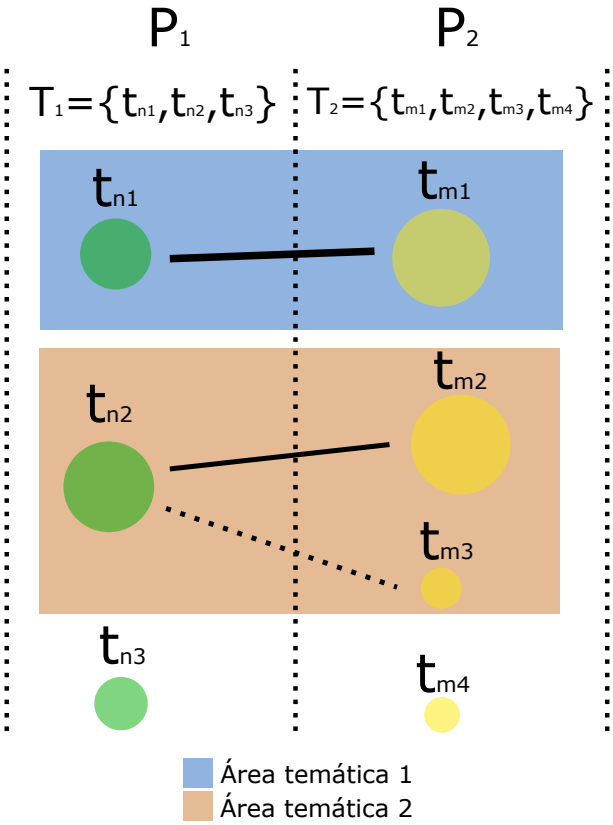


Figura 3.4: Mapa de evolución temporal.

de cómo se calcula este índice entre dos subperiodos sucesivos. Las esferas contienen los elementos (palabras clave) que corresponden a cada subperiodo. En la arista horizontal se observa el número de elementos compartidos por sendos subperiodos, es decir, $E_t \bigcap E_{t+1}$. En la arista oblicua ascendente (subperiodo t) se observa el número de elementos presentes en t que no se comparten con $t+1$, es decir, $E_t \setminus E_{t+1}$. Por último, en la arista oblicua descendente (subperiodo t+1) se observa el número de elementos que se incorporan nuevos al $t+1$, es decir, $E_{t+1} \setminus E_t$.

3.2 Revisión bibliográfica de la Literatura

Existen multitud de trabajos relacionados con la seguridad en redes. Por lo que para la extracción de la información necesaria para realizar este documento, se ha seguido una metodología concreta, obtenida del trabajo realizado por Kitchenham *et al.* [36].

En el inicio de cualquier investigación subyace la necesidad de identificar, medir y comprender lo que se ha hecho antes dentro de un área temática. Existen diferentes maneras de realizar una revisión bibliográfica de la Literatura aunque ciertamente no todas siguen una estructura o metodología que ayude a la revisión. Es por esto que se hace necesaria la utilización de herramientas o métodos que guíen en cierta forma la manera de proceder a la hora de realizar una revisión del estado del arte en un determinado tema. Este tipo de métodos se conocen como revisiones sistemáticas de la Literatura, o Systematic Literature Review (SLR), de sus siglas en inglés.

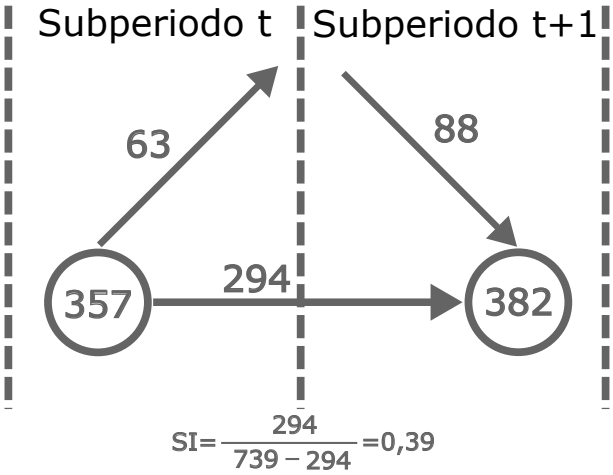


Figura 3.5: Esquema para el cálculo del Índice de Estabilidad entre subperiodos consecutivos.

Fueron Kitchenham *et al.* [35] [36] los que sentaron unas bases de estandarización para realizar estos procesos. A través de una SLR se puede estudiar el estado del arte de un tema, sus beneficios y limitaciones, se pueden identificar nichos y retos de investigación, y así sugerir futuros avances; o también ayudar a respaldar (contradecir) una hipótesis (antítesis). La premisa de la que parte este tipo de metodologías es que una revisión de la Literatura debe ser exhaustiva y justa, siendo esta la razón de hacerlo de una manera sistemática con pautas bien definidas. Una SLR debe ser capaz de encontrar la investigación que respalda la hipótesis, así como la que no lo hace. Cuando se hace una revisión sistemática previa, es menos probable llegar a resultados sesgados. Sin embargo, la desventaja de la utilización de este tipo de metodologías es que exige un mayor esfuerzo previo.

Una revisión sistemática deberá comenzar definiendo un protocolo de revisión que centre la(s) pregunta(s) de investigación que se abordará(n), así como la metodología que se usará. Como se ha comentado anteriormente, a través de una estrategia de búsqueda bien definida previamente, se intentará localizar el mayor número de trabajos posible en torno a la temática de estudio. Dicha estrategia de búsqueda quedará documentada durante el proceso con ánimo de evaluar la integridad y ofrecer un marco para su reproducibilidad. Además, la búsqueda debe tener criterios de inclusión y exclusión. Los datos numéricos son importantes para cualquier intento de resumir los resultados de un conjunto de Estudios primarios[2] y son un requisito previo para el Meta análisis[3] (es decir, técnicas estadísticas destinadas a integrar los resultados de los estudios primarios). Los resúmenes de estudios primarios se conocen como Estudios secundarios[4].

La comunidad científica en general está ampliamente de acuerdo sobre las fases principales a abordar durante una revisión sistemática, que son: (i) planificación de la revisión, (ii) realización de la revisión e (iii) informe de la revisión. Cada una de las fases fraccionable en sub-tareas, como identificar la necesidad de la revisión o plantear la pregunta de investigación durante la planificación. En la Figura 3.6 se muestra un diagrama de flujo del proceso principal de una

[2]Estudio primario. Un estudio empírico que trabaja en una pregunta de investigación específica.

[3]Meta análisis. Una forma de estudio secundario donde la síntesis de investigación se basa en métodos estadísticos cuantitativos.

[4]Estudio secundario. Un trabajo que revisa todos los estudios primarios posibles, con el objetivo de integrar/sintetizar evidencia relacionada con una pregunta de investigación específica.

revisión sistemática de la Literatura, centrado en la segunda etapa principal y sus sub-tareas. La fase que atañe a este trabajo se centra en la realización de la revisión. Kitchenham *et al.* [36], enmarca las sub-tareas descritas a continuación en esta fase:

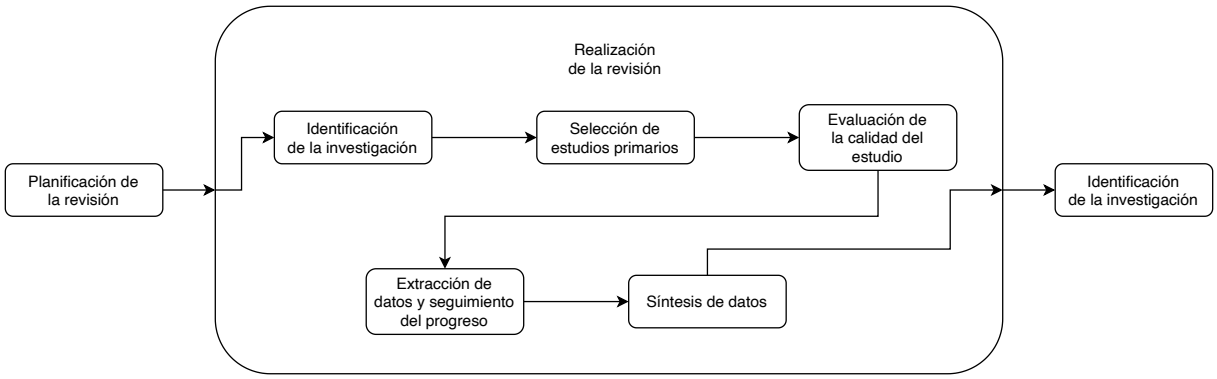


Figura 3.6: Principales etapas para la realización de la revisión del estado del arte mediante un enfoque SLR.

Identificación de la investigación. El objetivo de una revisión sistemática es encontrar tantos estudios primarios relacionados con la pregunta de investigación como sea posible utilizando una estrategia de búsqueda imparcial. El rigor del proceso de búsqueda es un factor que distingue las revisiones sistemáticas de las revisiones tradicionales.

Siguiendo una estrategia de búsqueda conjunta con personal bibliotecario experto, estas estrategias suelen ser iterativas, a través de búsquedas de revisiones preexistentes, evaluación del volumen de estudios potencialmente relevantes, realizar búsquedas probando diferentes términos derivados de la(s) pregunta(s) de investigación, y por supuesto, consultas a expertos en el tema.

Como comienzo, se puede dividir la pregunta en diferentes facetas como población, intervención, comparación, resultados, contexto, diseños de estudio. A continuación, se puede elaborar una lista de palabras que pueda contener sinónimos, abreviaturas y ortografías alternativas, también se pueden tener en cuenta encabezados y títulos de la materia usados en revistas y bases de datos. Una vez hecha una o varias cadenas de búsquedas, se pueden hacer más sofisticadas añadiéndoles operadores booleanos de tipo *AND* y *OR*.

Todo el proceso debería ser replicable, teniendo en cuenta que los estudios obtenidos cambiarán con el tiempo, y dependiendo de la disciplina en la que nos encontremos, lo harán más o menos rápido. Dicho lo cual, la revisión debe documentarse convenientemente, con la idea de que los lectores puedan evaluar la meticulosidad de la búsqueda.

Selección de estudios primarios. Una vez que se han obtenido los estudios primarios potencialmente relevantes, deben evaluarse para determinar su relevancia real.

A través de esta selección de estudios, se intentarán identificar aquellos que proporcionan evidencia directa sobre la cuestión de investigación. Para tratar de reducir el sesgo, se deben establecer los criterios de selección con anterioridad, aunque pueden refinarse durante el proceso. Del mismo modo, los criterios de inclusión/exclusión deben basarse en la pregunta de investigación, probándolos en varias búsquedas para garantizar su interpretación, es decir, se clasifiquen como se espera.

Se trata de un proceso parcelable en etapas, en el que se pueden interpretar unos criterios iniciales libres, de manera que, a menos que un estudio sea claramente excluible solo con leer titulo o resumen, lo ideal es obtener copias completas, para acceder a meta-datos como idioma, revista, autores, diseño de la investigación, metodologías, fecha de publicación, resultados y conclusiones, etc., que ayuden a discernir la bondad de un estudio. Las búsquedas electrónicas iniciales dan como resultado un gran número de documentos totalmente irrelevantes, es decir, documentos que no solo no abordan ningún aspecto de las preguntas de investigación, sino que ni siquiera tienen nada que ver con la disciplina.

Con toda la información, es una buena praxis mantener una lista de estudios excluidos que identifiquen el motivo, y mantener un registro de los estudios primarios candidatos que se excluyen como resultado de los criterios de inclusión/exclusión más detallados.

A la hora de incluir/excluir, un investigador individual, como puede ser un estudiante de doctorado, debería acudir a su supervisor para discutir dudas. A su vez, es adecuado realizar pruebas posteriores para evaluar una muestra aleatoria de estudios primarios para verificar sus decisiones de inclusión/exclusión.

Evaluación de la calidad del estudio. Además de los criterios generales de inclusión/exclusión, se considera crítico evaluar la "calidad" de los estudios primarios.

A través de una evaluación más minuciosa se obtienen criterios de inclusión/exclusión más detallados. Por ejemplo, averiguar si las diferencias de calidad explican las diferencias de los resultados de los estudios, cuantificar la importancia de los estudios individuales de forma acorde a su calidad, encaminar la interpretación de los resultados y orientar sugerencias para futuros trabajos, etc. Aunque no existe una definición acordada para la *calidad*, expertos del trabajo [59] sugieren que se relaciona directamente con minimizar el sesgo y maximizar la validez interna y externa.

Por norma general, las evaluaciones de calidad detallada se basan en listas de factores que se revisan para cada estudio, que se conocen como *instrumentos de calidad*. Por ejemplo, el índice-h que se basa en la cantidad de citas recibidas por un trabajo. Este dato sobre el *instrumento de calidad* es importante definirlo previamente, especificando como se usarán estas medidas para ayudar a seleccionar los estudios, elaborando criterios detallados de inclusión/exclusión o para ayudar al análisis de los datos extraídos, identificando subconjuntos de estudios que expliquen diferencias de calidad. Lógicamente, estas dos formas de usar las medidas de calidad no son excluyentes.

Extracción de datos y seguimiento del progreso. En la mayoría de los casos, la extracción de datos definirá un conjunto de valores numéricos que deben extraerse para cada estudio, como puede ser el número de citas (las que realiza y en las que aparece un estudio). Los datos numéricos son importantes para cualquier intento de resumir los resultados de un conjunto de estudios primarios y son un requisito previo para el meta análisis.

Si es posible, todos los documentos deberán ser revisados por varias personas, al menos dos, para realizar la extracción de datos por separado y poder comparar y discutir puntos que no queden claros, ya sea por consenso entre los investigadores o por el arbitraje de un investigador independiente adicional. Debido a limitaciones de tiempo o recursos, suele ser más común, que

varios investigadores se dividan el trabajo y cada uno extraiga los datos a un subconjunto de estudios primarios. En estos casos es importante emplear algún método para verificar que los investigadores extraigan datos de manera consistente. Se podría preparar una muestra aleatoria más pequeña que sí sea revisada por todos. De esta forma se evaluaría la consistencia entre investigadores.

Si se trata de un investigador individual, como un estudiante de doctorado, sería necesario, por ejemplo, que acuda nuevamente a su supervisor para que analice una muestra aleatoria. Por otro lado, también podrá realizar más pruebas usando diferentes muestras aleatorias del mismo conjunto principal, para hacer más efectivas y eficientes su propias verificaciones.

Se debe tener cuidado con las publicaciones duplicadas, es decir, un mismo estudio puede haberse publicado en diferentes revistas, y de alguna forma tener meta-datos diferentes como puede ser algún código identificativo propio de la fuente. Llegado el caso, puede ser necesario contactar directamente con el autor(es) para confirmar dicha duplicidad, si es cierta, se debe usar las más completa, pero podría ser necesario consultar la(s) descartada(s) para obtener más información.

Síntesis de datos. La síntesis de datos implica recopilar y resumir los resultados de los estudios primarios incluidos. La síntesis puede ser descriptiva (no cuantitativa). Sin embargo, a veces es posible complementar una síntesis descriptiva con un resumen cuantitativo. El uso de técnicas estadísticas para obtener una síntesis cuantitativa se denomina meta análisis.

La información extraída se debe estructurar para su lectura y análisis de la forma más cómoda posible, siendo coherente con la pregunta de investigación, como por ejemplo en tablas, tratando de resaltar similitudes y diferencias entre estudios. Es importante identificar el grado de homogeneidad entre los resultados extraídos de diferentes estudios, es decir, si al compararlos son consistentes, agregando la información a las tablas resultantes.

3.3 Herramientas

Se detallan a continuación las distintas herramientas y tecnologías que se han utilizado para la realización de esta investigación, describiendo brevemente cada una y justificando su uso.

DB Browser for SQLite

DB Browser for SQLite (DB4S) es una herramienta de código abierto para crear, diseñar y editar archivos de bases de datos compatibles con SQLite. También es multiplataforma.

Justificación de uso

La aplicación *SciMAT* trabaja en su *Backend* con una Base de Datos (BD) en *SQLite*, y a veces es necesario hacerle alguna consulta directamente a la base de datos. DB4S es simple, fácil de usar, al tratarse de *SQLite*, no necesita instalación de servicios extra, ya que se trabaja con ficheros binarios especificos de esta tecnología.

diagrams.net

diagrams.net es un marco para diseño de diagramas de todo tipo, Unified Modeling Language (UML), Business Process Model and Notation (BPMN), diagramas de flujo, etc. Es *OpenSource*, y multiplataforma, además se puede usar tanto con versión de escritorio como web, y se acopla perfectamente con la nube.

Justificación de uso

Es una aplicación muy sencilla de usar, existen alternativas más potentes como puede ser *Visual Paradigm*. Sin embargo *diagrams.net* es ligera e intuitiva, no necesita registros, y al conectarse perfectamente con *Google Drive* (almacenamiento en la nube elegido para compartir todo el material del proyecto) es la opción más aconsejable.

Documentación

Portable Document Format (PDF) («formato de documento portátil»), es un formato de almacenamiento para documentos digitales independiente de plataformas de software o hardware. Este formato es de tipo compuesto (imagen vectorial, mapa de bits y texto).

Justificación de uso

Al estar considerado como un estándar, es muy fácil de leer, cualquier navegador tiene integración con este formato, por lo que hace casi innecesario realizar cualquier cambio en la máquina donde se intente leer un documento en este formato. Además, este formato es capaz de portar fácilmente texto, imágenes, tablas, etc.

Email

Mozilla Thunderbird es un cliente de correo electrónico multiplataforma, *OpenSource*, desarrollado por la Fundación Mozilla. Utiliza el lenguaje de interfaz XML User Interface Language (XUL) y viene instalado por defecto en los sistemas de escritorio de diversas distribuciones Linux.

Justificación de uso

La comunicación con las personas relacionadas con el proyecto; directores, tutores, colaboradores, etc. Habría sido muy complicada si dependiera en exclusiva de reuniones en físicas. El correo electrónico es de gran ayuda en estas situaciones ya que aporta una comunicación asíncrona con histórico de conversaciones. En general se ha usado *Thunderbird*, pero también se ha usado el cliente de *Microsoft Outlook*.

GanttProject

GanttProject es una aplicación *OpenSource* y Multiplataforma escrita en Java que permite la planificación de proyectos de una forma muy simple e

intuitiva a través de diagramas de Gantt.

Justificación de uso

Este proyecto no tiene una gran planificación con mucha carga de tareas distintas, ni tampoco con recursos que gestionar para cada tarea, por lo que *MS Project*, por ejemplo, es una aplicación demasiado poderosa para aplicarla, en cambio *GanttProject*, que también posee características para manejar tareas y recursos, es bastante más simple, y nos ayuda en este caso de un proyecto no muy complejo, a planificarlo de una manera más concreta.

GIMP

GNU Image Manipulation Program (GIMP) es un editor de imágenes multiplataforma de código abierto. Proporciona herramientas sofisticadas para la edición de imágenes.

Justificación de uso

El famoso programa de manipulación de imágenes de código abierto se ha usado para la edición de algunas de las imágenes a lo largo de este documento. Es intuitivo y fácil de usar si se tiene un mínimo de conocimientos, y muy conocido por los miembros del proyecto, por lo que se ha elegido esta herramienta en lugar de otros editores y manipuladores de imágenes.

Git

Git es un software para control de versiones de repositorios distribuidos, es de código abierto, muy sencillo de implementar y de usar, pero muy útil y potente en un entorno de desarrollo de software, aunque permite gestionar versiones de cualquier tipo de fichero en un computador, según la documentación oficial[5]:

> *"Git es un sistema de control de versiones distribuidas de código abierto y gratuito diseñado para manejar todo, desde proyectos pequeños a muy grandes, con velocidad y eficiencia."*

> *"Git es fácil de aprender y tiene una huella pequeña con un rendimiento increíblemente rápido. Supera a las herramientas de SCM como Subversion, CVS, Perforce y ClearCase con funciones como ramificación local barata, áreas de preparación conveniente y flujos de trabajo múltiples."*

Justificación de uso

[5] https://git-scm.com

La elección de *Git* como gestión del control de versiones es además de por el conocimiento de la tecnología, como dice su documentación, Git es muy eficiente desde el punto de vista de los recursos de la máquina, puesto que no necesitamos desplegar ningún servicio si no es necesario, y es muy intuitivo desde el punto de vista de la experiencia de usuario. Si a su uso agregamos algún cliente con interfaz gráfica su capacidad de información visual se incrementa notablemente.

Google Drive

Google Drive es un servicio de almacenamiento y sincronización de archivos desarrollado por Google, permite a los usuarios almacenar archivos en sus servidores, sincronizar archivos entre dispositivos y compartir archivos entre usuarios.

Justificación de uso

Las cuentas institucionales de la Universidad de Almería, así como la de Cádiz, de las que disponen todos los miembros del equipo, tienen acceso a los servicios del gigante californiano, como *Gmail*, *Google Drive*, *Google Cloud*, etc. trabajar y compartir con la nube de Google es sencillo y rápido.

Inkscape

Es un editor profesional de vectores gráficos multiplataforma. Es *OpenSource*.

Justificación de uso

Las imágenes vectoriales son mucho más maleables y fáciles de adaptar a diferentes tamaños, además de que fabricando nuestras propias imágenes y gráficos evitamos problemas de derechos de autor. Al igual que GIMP también es de *OpenSource*, intuitivo y cómodo, y conocido por todos los miembros del proyecto.

LaTeX

Es un sistema de composición de textos, orientado a la creación de documentos escritos que presenten una alta calidad tipográfica. Por sus características y posibilidades, es usado de forma especialmente intensa en la generación de artículos y libros científicos que incluyen, entre otros elementos, expresiones matemáticas.

Justificación de uso

LaTeX se ha convertido en un estándar a la hora de redactar textos científicos (o de investigación en general), se adapta muy bien a la inclusión de gráficos, tablas, formulas matemáticas, etc. Además, existen en el mercado potentes editores, tanto para trabajar en local como en remoto, lo que lo hace ideal a la hora de colavorar para escribir cualquier documento.

Mendeley

Mendeley es una aplicación web y de escritorio, propietaria y gratuita (propiedad de Elsevier). Permite gestionar y compartir referencias bibliográficas y documentos de investigación, encontrar nuevas referencias y documentos y colaborar en línea

Justificación de uso

Gestor de referencias con plataformas online y local, es una herramienta de uso colaborativo para investigadores, con visor de PDF integrado, dando así la oportunidad de buscar, resaltar y compartir artículos de interés e información relevante dentro de los mismos. Además, dispone de una cómoda extensión para Google Chrome (y Firefox) que permite incorporar las referencias encontradas en la web directamente a nuestra biblioteca digital sincronizada con el cliente de escritorio.

NetBeans

NetBeans es un Integrated Development Environment (IDE) libre, hecho principalmente para el lenguaje de programación Java. Existe además un número importante de módulos para extenderlo. *NetBeans* IDE es un producto libre y gratuito sin restricciones de uso.

Justificación de uso

SciMAT es una aplicación para la que sus autores han dejado el código fuente alojado en su web, y se trata de un proyecto de este IDE, por lo que se ha usado para ver y adaptar algún detalle (en concreto del *Wizard*), y así tener nuestra compilación para hacer más cómodo nuestro uso propio.

Notas de iCloud (Evernote)

Notes es una aplicación para tomar notas desarrollada por Apple. Se proporciona en sus sistemas operativos iOS y macOS. Funciona como un servicio para hacer notas de texto cortas, que pueden sincronizarse entre dispositivos usando el servicio iCloud de Apple. *Evernote* es una aplicación cuyo objetivo es la organización de información personal mediante el archivo de notas. Ambas permiten su uso colaborativo.

Justificación de uso

Estas herramientas de apuntes colaborativas son especialmente útiles para tomar notas y apuntar ideas de forma rápida, y compartirlas con el resto del equipo de trabajo. Lo que permite mantener informados a todos los participantes de novedades, o posibles cambios que afecten al proyecto, además de permitir darle forma a las ideas para luego pasarlas a la documentación final.

Paquete Office

Microsoft Office es una suite ofimática que abarca el mercado completo en Internet e interrelaciona aplicaciones de escritorio, servidores y servicios para los sistemas operativos Microsoft Windows, Mac OS X, iOS y Android.

Justificación de uso

Gracias al Acuerdo Microsoft Office 365 ProPlus - UAL[6].

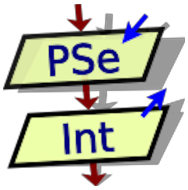
> *"Con la nueva licencia A3, además de las ventajas actuales, se dispondrá de acceso a nuevos servicios en el portal y la posibilidad de la instalación en 5 PCs o MACs, 5 dispositivos Tablets y 5 móviles y 1 TB de espacio en OneDrive."*

> *"Una vez finalizada su relación con la Universidad de Almería, podrá seguir accediendo a la plataforma de Microsoft con su usuario y contraseña, pero su licencia pasará a A1. No perderá ninguno de sus documentos, ni reducción de espacio en OneDrive. Pierde el uso de la versión de escritorio, es decir, la versión descargada e instalada en su dispositivo. Deberá entrar en el portal de Office 365."*

La comunidad universitaria puede hacer uso del Paquete Office. Es innegable que se trata de la suite ofimática por excelencia, y que desbanca a sus alternativas gratuitas. Se ha usado Excel para trabajar con tablas y datos, y exportar gráficas. Word para la redacción de diferente documentación asociada al proyecto. Powerpoint para la realización de la presentación de defensa de este trabajo. Y Outlook como cliente de correo electrónico.

PSeInt

PSeInt es una herramienta que, mediante un simple e intuitivo pseudolenguaje en español, abstrae la escritura de código fuente. Permite centrar la atención en los conceptos fundamentales de la algoritmia computacional.



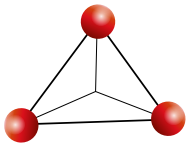
Justificación de uso

PSeInt es otra herramienta muy conocida en el ámbito de la programación, es sencilla, intuitiva y clara. Permite el diseño en las primeras etapas de nuevos

[6] Software para la comunidad universitaria

algoritmos, para exportarlos más tarde a códigos fuente como *C*, *C#*, *Java* o *Python*. Se trata de una herramienta muy versátil para un ingeniero de software.

SciMAT



SciMAT es una herramienta de software de código abierto (GNU General Public License (GPL) v3) desarrollada para realizar un análisis de *Science Mapping* bajo un marco longitudinal. *SciMAT* proporciona diferentes módulos que ayudan al analista a llevar a cabo los pasos del flujo de trabajo de *Science Mapping*.

Justificación de uso

El centro de este trabajo de investigación es un análisis bibliométrico de la Literatura referida a la disciplina de estudio, un mapeo de ese análisis a través de diagramas estratégicos y redes temáticas detectadas y una Revisión sistemática de la Literatura. *SciMAT* entra de lleno en buena parte de todo ese trabajo, se trata de una herramienta de código abierto desarrollada por el Dr. MJ Cobo en la Universidad de Granada. *SciMAT* es muy fácil de usar, los resultados obtenidos son una gran ayuda, es muy apropiada para programas de doctorado en las primeras etapas en las que se realizan estudios del estado del arte.

Skype

Es un software que permite comunicaciones de texto, voz y vídeo sobre Internet (Voice over IP (VoIP)) de forma gratuita. Es propiedad de Microsoft. El código y protocolo de Skype permanecen cerrados y son privativos de la aplicación, pero los usuarios interesados pueden descargar gratuitamente la aplicación ejecutable del sitio web oficial. Es multiplataforma.

Justificación de uso

Quizás nunca ha estado más justificado su uso durante un proyecto de este tipo. El equipo de trabajo ha necesitado estar en continuo contacto con reuniones por todas las semanas, algunas veces más de una vez por semana, lo cual hubiera sido absolutamente imposible sin una herramienta de estas características, se eligió *Skype* por el conocimiento de ella de todos los miembros del equipo, el cliente de escritorio es muy sencillo e intuitivo.

TeXstudio (Overleaf)

TeXstudio es un IDE específico para LaTeX que proporciona un soporte moderno de escritura, como la corrección ortográfica interactiva, plegado de código y resaltado de sintaxis. *Overleaf* es un editor colaborativo de LaTeX basado en la nube que se utiliza para escribir, editar y publicar documentos científicos.

Justificación de uso

El presente documento se ha escrito usando *LaTeX*, como ya se ha comentado,

Overleaf es una plataforma para escribir y alojar nuestros proyectos *LaTeX* perfecta, ya que ofrece la conexión a través de repositorios distribuidos *Git*, por lo que podemos editar tanto local como remotamente y sincronizar los cambios a traves de gestores destinados a esa tarea, como puede ser *Sourcetree* o el cliente de consola directamente.

SourceTree

SourceTree[7] es un cliente de la compañía Atlassian, para Git que dispone de interfaz gráfica.

> *"Un cliente Git gratuito para Windows y Mac. Sourcetree simplifica la forma en que interactúa con sus repositorios de Git para que pueda concentrarse en la codificación. Visualice y administre sus repositorios a través de la sencilla GUI de Git de Sourcetree."*

Justificación de uso

Por defecto, Git puede manejarse por comandos de consola, en Windows nos ofrece un cliente en modo texto que recuerda a una Shell de Unix, en Linux y macOS hace uso de la propia Shell de estos sistemas operativos. La elección del cliente *SourceTree* se debe al extenso conocimiento de su funcionamiento tras usarlo durante toda la carrera.

Sublime Text

Sublime Text es un moderno editor de texto con características especiales destinadas al resaltado de código e indentación del mismo, además de ofrecer herramientas de auto-completado que lo acercan a un IDE, sin dejar de ser un editor de texto.

Justificación de uso

Existen alternativas más simples como el bloc de notas de Windows, TexEdit de Mac, o incluso teniendo en cuenta que estamos hablando de texto plano, editores de texto por consola como Nano, estas opciones las descartamos por la magnitud de los documentos que estamos editando. Del otro lado están los editores modernos como *Visual Studio Code*, *Atom*, *Brackets*, de entre los cuales se eligió *Sublime Text* porque después de años utilizándolo ya es nuestro editor de texto para absolutamente todo, y porque no deja de ser simple de usar y a la vez potente.

Web of Science (bibliotecas digitales)

Una biblioteca digital es una colección de objetos digitales organizados, que sirve a una comunidad de usuarios definida, que tiene los derechos de autor presentes y gestionados y que dispone de mecanismos de preservación y conservación. Web of Science es un servicio en línea de información científica,

[7] Sourcetree | Free Git GUI for Mac and Windows

suministrado por Clarivate Analytics, integrado en ISI Web of Knowledge (WoK).

Justificación de uso

La *Web of Science* es accesible a través del proxy de la UCA, estando conectados a su Virtual Private Network (VPN), de esta forma se tiene acceso a todo el contenido que pueda proporcionarnos el *login* como institución educativa (según acuerdos entre la UCA o el Ministerio de educación y los distintos servidores de contenido bibliográfico digital). La biblioteca de la WoS permite exportar las búsquedas a documentos en texto plano, etiquetados con los distintos campos (título, autor, revista, palabras clave, fecha de publicación, citas, etc.) con formato ISIWoS, entre otros, formato que acepta la aplicación *SciMAT*. Otras bibliotecas digitales que se han usado son *Google Scholar*, *IEEE Xplore® digital library*, *ACM Digital Library*, *SpringerLink* y *Scopus*.

4. Estudio y análisis de la Literatura

En este capítulo se presenta el análisis del estado del arte sobre seguridad en redes *Ad hoc*. Para ello se ha realizado un estudio y mapeo bibliométrico detallado de *Áreas Temáticas* a través de la base de datos de WoS y el software *SciMAT*. A continuación se ha realizado una revisión sistemática de la Literatura (SLR) siguiendo las metodologías propuestas en [35] y [36]. Se han extraído los documentos que se han considerado relevantes. Finalmente, se presenta una nueva taxonomía que trata de solventar la falta de consenso y homogeneización en lo que respecta a las líneas de defensa.

4.1 Estudio bibliométrico y análisis de temáticas, tendencias y evolución

La base de datos utilizada para realizar el estudio bibliométrico es la WoS, puesto que es aceptada como motor principal en el entorno académico mundial y engloba publicaciones de otras bases de datos diferentes. Para seleccionar el conjunto de documentos se ha realizado una búsqueda metodológica por palabras clave sobre el tema, utilizando la terminología que ofrece la web. En la Figura 4.1 se ve la leyenda de las etiquetas de campo y operadores booleanos que se pueden usar para conformar una consulta en WoS. Según esta leyenda y las necesidades de nuestro estudio, se realizó una búsqueda general por tema con la etiqueta TS (Tema), que incluye búsquedas en los campos título, resumen y palabras clave, y centrado en el área de investigación con la etiqueta SU (Área de investigación). Para este trabajo concreto y esta parte del estudio, se acotó el periodo de búsqueda a la última década. En la Subsección 4.1.1 se detalla.

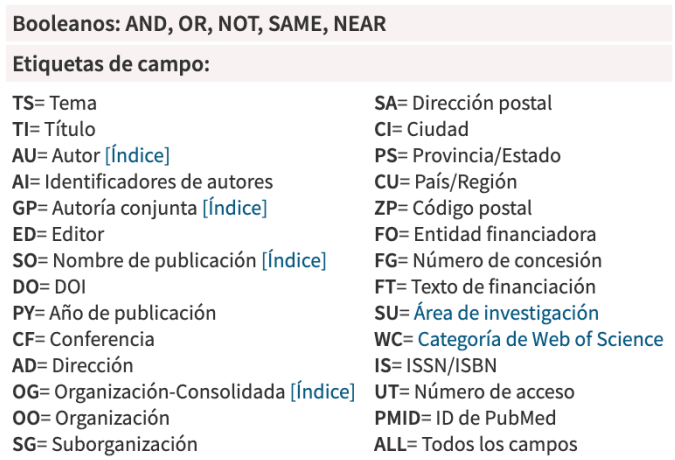


Figura 4.1: Etiquetas de campo y operadores booleanos para crear una consulta en WoS.

WoS también permite elegir las bases de datos en las que realizar la búsqueda. A continuación se muestran las que se han utilizado en este estudio (Tabla 4.1):

Tabla 4.1: Colección principal de Web of Science: Índices de citas

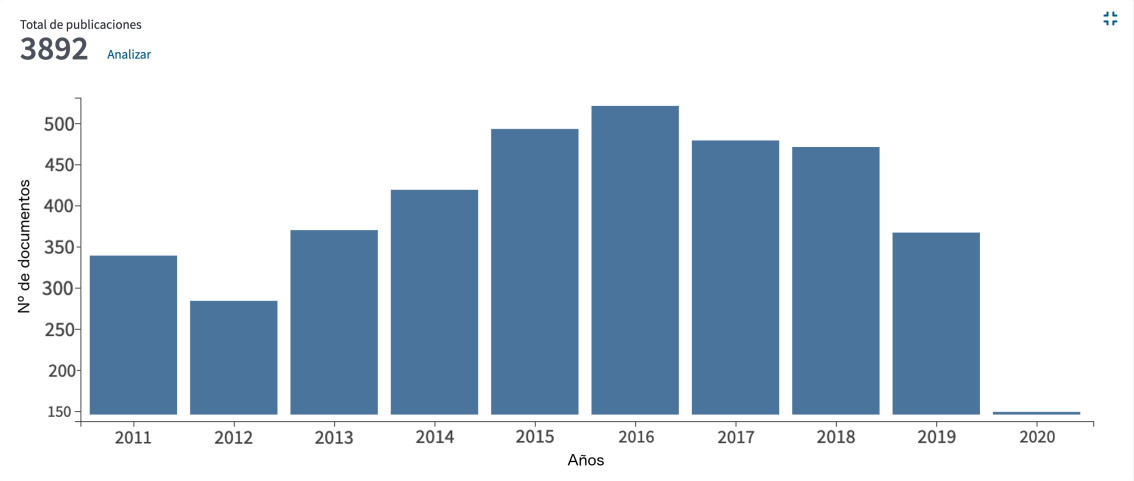
Collection	Desde	Hasta	Seleccionada
Science Citation Index Expanded (SCI-EXPANDED)	1900	Actualidad	✓
Social Sciences Citation Index (SSCI)	1956	Actualidad	-
Arts & Humanities Citation Index (A&HCI)	1975	Actualidad	-
Conference Proceedings Citation Index- Science (CPCI-S)	1990	Actualidad	✓
Conference Proceedings Citation Index- Social Science & Humanities (CPCI-SSH)	1990	Actualidad	-
Book Citation Index- Science (BKCI-S)	2005	Actualidad	✓
Book Citation Index- Social Sciences & Humanities (BKCI-SSH)	2005	Actualidad	-
Emerging Sources Citation Index (ESCI)	2005	Actualidad	✓

Para la obtención de los resultados se ha llevado a cabo la siguiente búsqueda con el siguiente patrón:

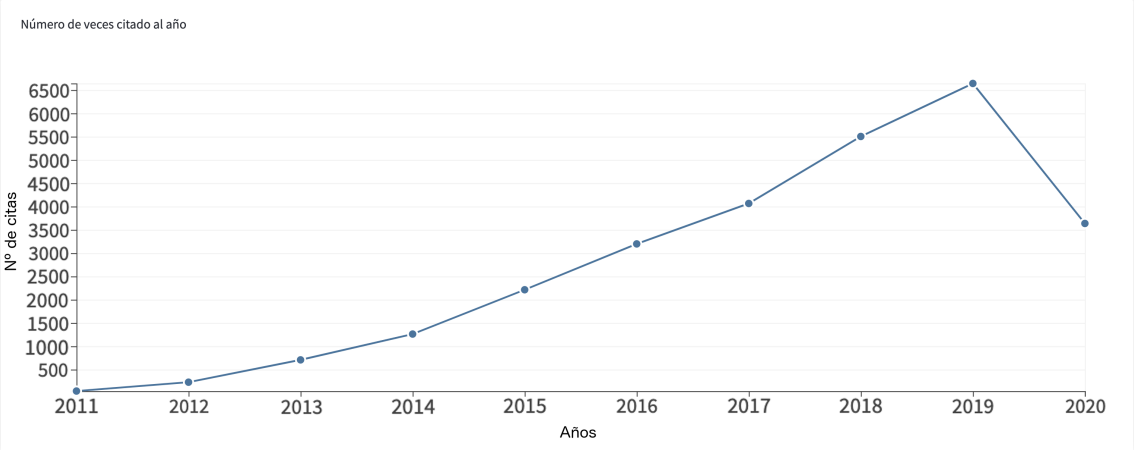
```
1  TS=(security AND "ad hoc") AND SU=(Engineering OR Computer Science)
```

Esta consulta devolvió unos 4000 resultados entre los años 2011 y 2020. Aunque se puede afinar más estableciendo filtros para extraer solo resultados que correspondan a tipos de documentos, como pueden ser artículos o conferencias, se ha decidido no hacerlo para obtener la máxima información sobre lo que se esta investigando en la disciplina a tratar.

La propia aplicación web nos permite extraer unos primeros datos relevantes. Por ejemplo, la posibilidad de agrupar el número de documentos obtenidos por año (Subfigura 4.2(a)) o poder realizar un informe de citas (Subfigura 4.2(b)), con los que esbozar un breve *Análisis de Rendimiento* bibliométrico. Tras analizar dichas figuras, se observa claramente un pico de estudios en los años 2015 y 2016. Sin embargo, el número de citas sigue en aumento durante los siguientes años, tanto en 2017, 2018 y 2019, de lo que se puede inferir que el estudio en el campo de la seguridad en este tipo de redes sigue activo.



(a) Documentos por año.



(b) Cantidad de citas por año.

Figura 4.2: Gráficos de publicaciones obtenidos de la WoS. En la Subfigura 4.2(a) vemos documentos por año de publicación. En la Subfigura 4.2(b) vemos citas por año publicación.

Seguidamente se describe la metodología explicada a través de la Figura 4.3. Se trata de un diagrama de flujo que detalla los procesos y subprocesos comentados en la Sección 3.1, junto a la Figura 3.2. Como se puede observar, se trata de un proceso iterativo de revisión del análisis, que pasamos a detallar a continuación.

A partir de la búsqueda anterior, se descargó la información de la base de datos WoS en forma de *Dataset* en texto plano con todos los meta datos de cada artículo[1]. En la Tabla 4.2 se

[1] Instrucciones para la extracción y descarga de los registros.

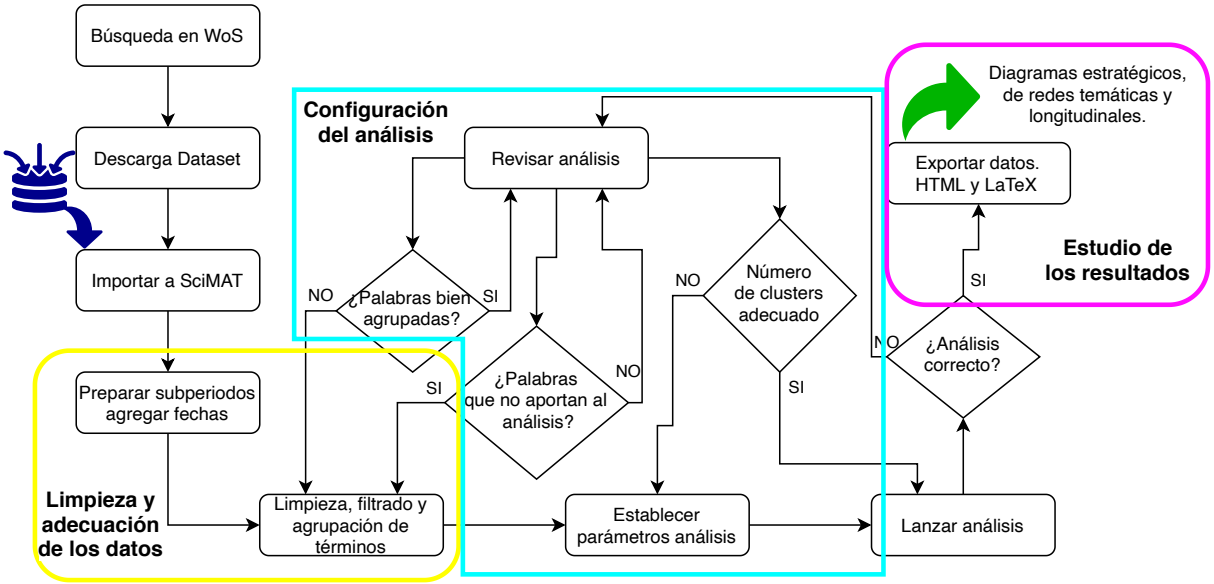


Figura 4.3: Diagrama de flujo del proceso de toma de datos e incorporación a SciMAT para su análisis.

puede ver un resumen de la estructura del *Dataset*. Se han omitido algunos campos[2] para mayor claridad. *SciMAT* trabaja con los campos DE, ID, TI, CR, DA, SO, AU, AF. Estos son los más relevantes para realizar cualquier tipo de análisis, ya sea de co-palabras, de co-citas, análisis de autorías, etc. En este trabajo, como se realiza un análisis de co-palabras, se utilizan dos tipos de *keywords* (campos DE e ID). A partir del *Dataset* anterior y con ayuda de la herramienta *SciMAT* se procederá al estudio de los principales temas y tendencias en la Literatura relacionada.

Tabla 4.2: Esta tabla contiene algunos de los campos de la estructura del *dataset* descargado de WoS.

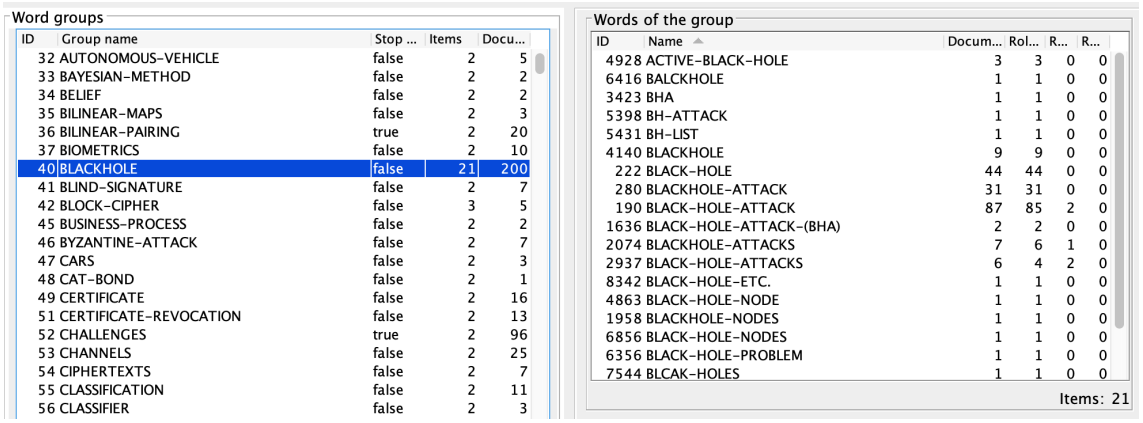
Nombre de Etiqueta	Significado
FN	Inicio del fichero
VR	Versión del formato del fichero
PT	Tipo de publicación
AU	Autor
AF	Autor completo
TI	Título
DE	Palabras clave del autor
ID	Keyword Plus (WoS key words)
CR	Referencias citadas
SO	Fuente - Revista
DA	Fecha
...	- CAMPOS OMITIDOS -
ER	Fin del elemento
EF	Fin del fichero

[2]Para más información, consultar la Ayuda de la Colección principal de Web of Science.

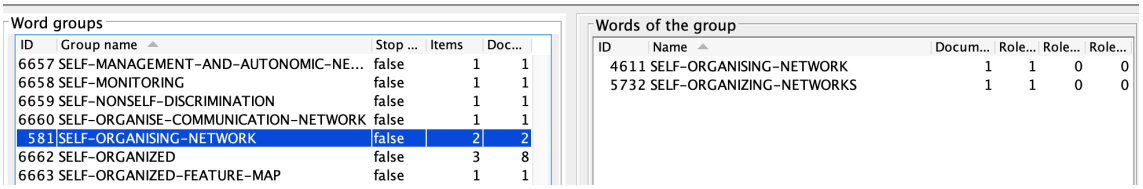
4.1.1 Limpieza y adecuación de los datos

Se ha decidido acotar la búsqueda a los años 2011 - 2020 (última década), y dividirlo en dos subperiodos: (2011 - 2015) y (2016 - 2020), como aconseja la aplicación *SciMAT*. Así, se podrán estudiar ambos subperiodos por separado y analizar la evolución de las temáticas a lo largo de esos años.

La primera fase del estudio con esta aplicación bibliométrica pasa por limpiar y filtrar los términos usados como palabras clave. Para el conjunto de datos que se usó existían más de 8000 términos distintos, muchos de los cuales son plurales. Además existen palabras distintas para el mismo concepto, por lo que es necesario hacer un agrupamiento de términos. En la Figura 4.4 se puede ver como se agrupan los términos, con un ejemplo de agrupación que englobaría muchas palabras clave (Subfigura 4.4(a)), y otro que solo incorpora el singular y el plural de la misma cosa (Subfigura 4.4(b)).



(a) Grupo de palabras clave masivas



(b) Grupo de palabras clave singular/plural

Figura 4.4: Ejemplo de agrupación de términos clave en SciMAT. En la Subfigura 4.4(a) se ve la agrupación de palabras clave que hacen referencia al ataque *Black Hole*. En la Subfigura 4.4(b) se ve el grupo de palabras para las redes autoorganizadas.

4.1.2 Configuración del análisis

Una vez agrupadas todas las palabras clave, se realiza el análisis, siguiendo los fundamentos teóricos de la Subsección 3.1. En la Figura 4.5 se muestra un diagrama de flujo con los sucesivos pasos seguidos a través del *Wizard* de *SciMAT*.

Primero se seleccionan los dos periodos mencionados, y a continuación, el tipo de análisis que se va a realizar. En este caso se va a hacer un análisis de co-palabras, por lo que se selecciona como unidad a analizar *word* y se marcan las casillas del autor y de la Fuente (revista). La

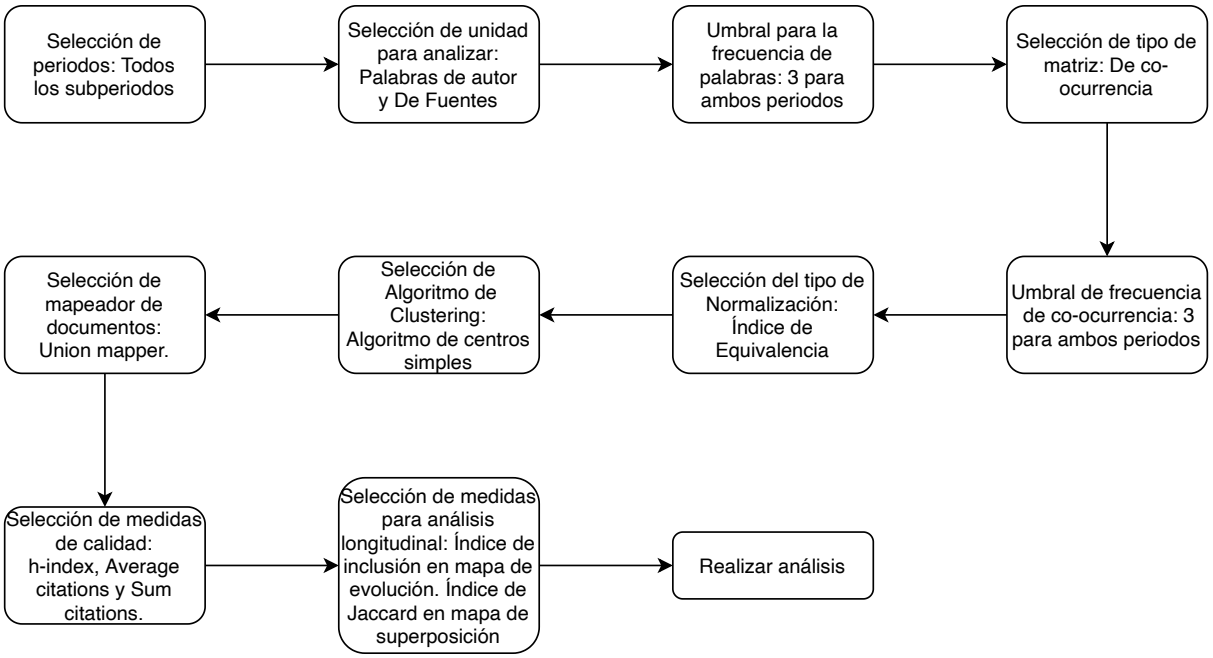


Figura 4.5: Diagrama de flujo del proceso de selección de parámetros de SciMAT.

frecuencia de repetición de palabras se establece a 3, es decir, debe aparecer al menos en 3 documentos. El tipo de matriz es de co-ocurrencia, para realizar el análisis de co-palabras. El límite para las aristas también se establece a 3, lo que significa que dicha co-ocurrencia no puede ser menor a 3. Para la normalización se selecciona el Índice de equivalencia como medida de similitud. Cómo algoritmo de clusterización se usa el de centros simples con umbrales máximo de 8 y mínimo de 4. Cómo mapeador de documentos se selecciona el *union mapper*. Cómo medidas de calidad se usan el índice-h y el número de citas. Para el análisis longitudinal temporal se selecciona el Índice de Inclusión para el mapa de evolución y el Índice Jaccard para el mapa superpuesto. Estos parámetros son los recomendados por los creadores de *SciMAT* para este tipo de análisis.

Los mapas y diagramas resultantes del análisis realizado por periodos se muestran y analizan a continuación. Diferenciaremos así entre diagramas estratégicos, redes temáticas y análisis longitudinal. Las subsecciones a continuación comprenden la etapa “Estudio de los resultados” de las correspondientes Figuras 3.2 y 4.3.

4.1.3 Análisis del periodo 2011 - 2015

Se muestran a continuación los diagramas estratégicos para el conteo de documentos (Subfigura 4.6(a)) y el índice-h (Subfigura 4.6(b)) del primer subperiodo.

En esas figuras se observan como temáticas motor: VANET, BLACKHOLE e IDS. Además, se aprecia perfectamente la posición para el que sería el concepto general de redes de sensores *Ad hoc* como temática transversal, temática dentro de la que se habla de muchos subtemas que no tienen por que estar relacionados entre ellos. Según la disposición observada en estos diagramas y la información extraída para las medidas cuantitativas (Tabla 4.3), se hace notable la temática BLACKHOLE puesto que incluye al tema MANET, fuertemente relacionado con lo que parece

(a) (b)

Figura 4.6: Diagramas estratégicos del primer subperiodo (2011 - 2015). En la Subfigura 4.6(a) se ve el diagrama estratégico correspondiente al conteo de documentos, mientras que en la Subfigura 4.6(b) se observa el equivalente para el índice-h.

haber sido el punto débil de este tipo de redes *Ad hoc* durante esos años. El *Packet Dropping* esta presente en el contenido de este cluster, así como el protocolo de enrutamiento clásico que sufre este ataque, el AODV. Ver Figura 4.7(a). Estos temas del primer periodo tienen un alto número de citas, sobre todo los temas VANET y BLACKHOLE, con un Índice-h alto, que los corrobora como temas motor (sin perder de vista el hecho de que BLACKHOLE incluye a MANET).

La temática WIRELESS-AD-HOC-SENSOR-NETWORK en estos años aparece en el cuadrante de obsoletas/nuevas, sin embargo obtiene un índice-h elevado en relación a las demás temáticas detectadas y un alto número de citas. Además, incluye temas que resultan básicos y transversales como REPUTATION, TRUST-MODEL, SECURITY-ATTACKS, y mención especial merece el tema GENETIC-ALGORITHM-(GA).

Tabla 4.3: Medidas de rendimiento de los grupos del periodo 2011 - 2015.

Nombre del tema	Número de documentos	Índice-h	Promedio de citas	Número de citas
VANET	486	43	14,85	7.215
BLACKHOLE	719	30	5,83	4.194
WIRELESS-AD-HOC SENSOR-NETWORK	164	28	20,76	3.405
ROUTING-PROTOCOL	304	25	9,36	2.845
IDS	138	22	14,69	2.027
WORMHOLE	141	14	7,3	1.029
ASYMMETRIC-CRYPTOGRAPHY	70	12	5,36	375

ROUTING-PROTOCOL también se postula como temática transversal, tiene un índice-h más bajo, pero si un alto número de citas. Otra temática que merece mención en este periodo es la de ASYMMETRIC-CRYPTOGRAPHY, que parece ser un tema aislado, de lo que se deduce que se relaciona poco con otras temáticas. Como se aprecia en la misma Tabla 4.3 esta temática ha obtenido pocas citas en este periodo.

En cuanto a las redes temáticas, en las Subfiguras 4.7(a), 4.7(b) y 4.7(c) se pueden ver las de los temas motor del primer periodo. Como decíamos anteriormente, la temática BLACKHOLE (Subfigura 4.7(a)) incluye MANET, AODV (protocolo clásico en MANET) así como temas relacionados con el *Packet Dropping*, lo que pone de manifiesto como se ha volcado la investigación en sofocar esta amenaza principalmente en el contexto de las MANET.

En la red temática de VANET (Subfigura 4.7(b)) se puede ver que se relaciona con temas de privacidad y seguridad en los protocolos, y se establece una conexión única entre VANET y ROAD-SIDE-UNIT-(RSU), que muestra su dependencia.

La red temática de IDS (Subfigura 4.7(c)) muestra poca interconexión interna, se trata de una temática que se relaciona con temas no co-relacionados entre ellos, salvo entre CELLULAR-LEARNING-AUTOMATA y GLOMOSIM-SIMULATOR por un lado, e IDS-ARCHITECTURES y SECURITY-VULNERABILITIES por otro. En esos casos si que existe una fuerte co-relación entre ambas parejas, y es precisamente lo que hace situarse a esta temática en una zona tan alta desde el punto de vista de la densidad (ver Figura 4.6). Aun y así, esta red tiene un cariz más de temática transversal que de tema motor, por la desconexión general de sus nodos componentes.

Los temas transversales del primer periodo, de los cuales se pueden ver sus redes temáticas en las Figuras 4.8(a) y 4.8(b). En dichas redes podemos observar el parecido con la red temática de IDS. WIRELESS-AD-HOC-SENSOR-NETWORK y ROUTING-PROTOCOL son temáticas mencionadas en la mayoría de documentos analizados, pero sin que tengan relación directa, por eso aparecen junto a términos dispares que tampoco se relacionan, es decir, que aparecen junto a la temática central únicamente.

Las últimas temáticas del primer periodo son temas aislados y se comentan a continuación. WORMHOLE como amenaza de capa 3 que afecta también a protocolos como AODV, reafirmando lo vulnerable que son las redes *Ad hoc* frente a este tipo de amenazas. ASYMMETRIC-CRYPTOGRAPHY se relaciona en este periodo con su algoritmo de encriptado por excelencia, Rivest Shamir Adleman (RSA) [60] y con otras tecnologías criptográficas. Por el cuadrante donde está se puede ver que es una temática especializada. Sin embargo, por su baja densidad no se ha usado mucho en este periodo en las redes *Ad hoc*.

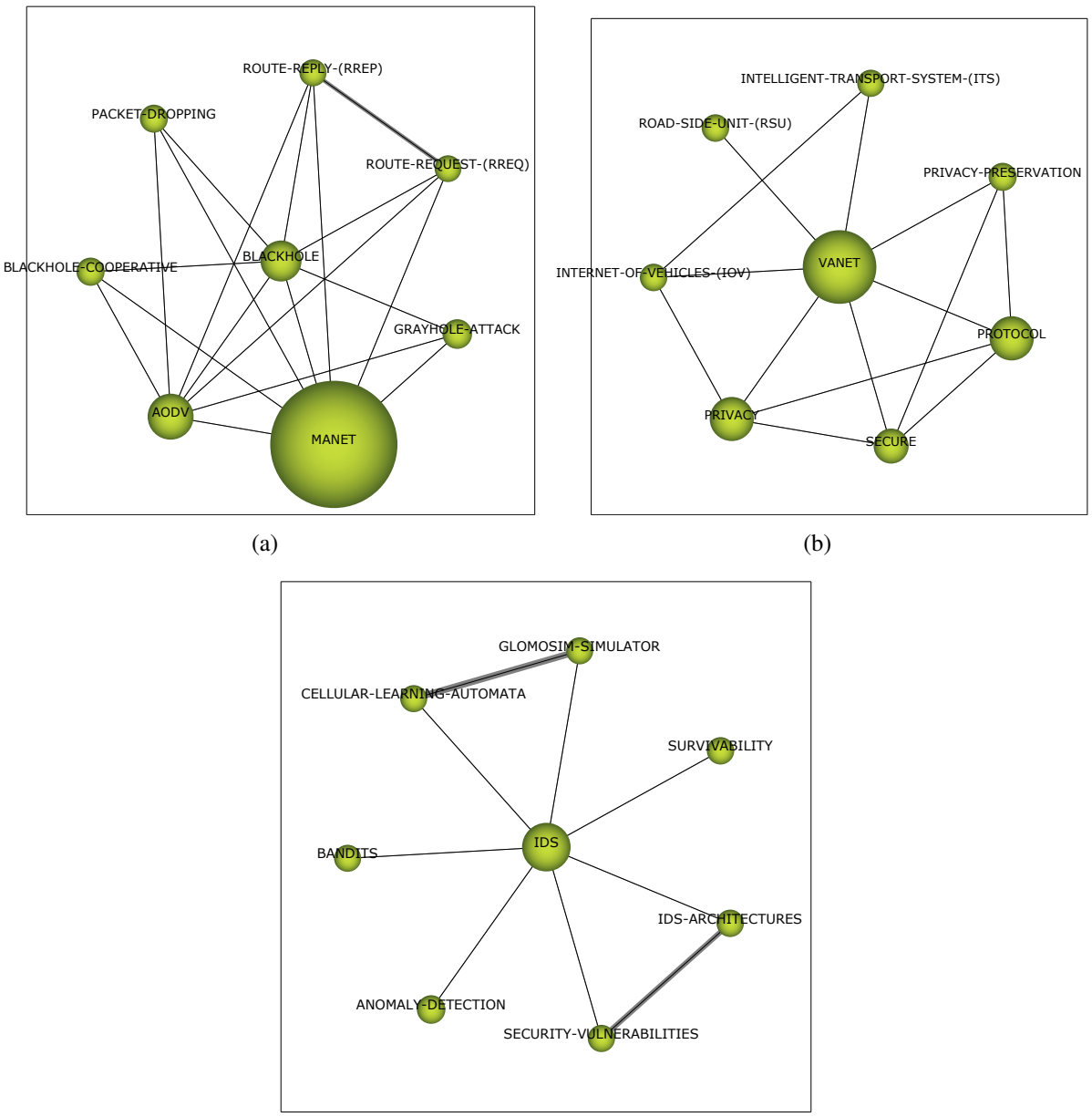


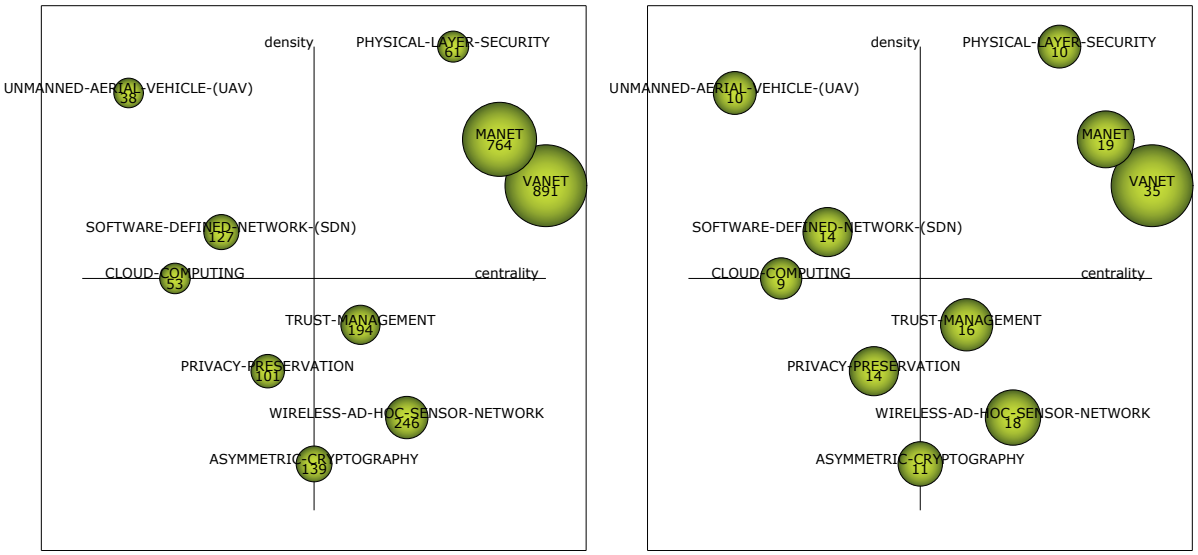
Figura 4.7: Redes temáticas del primer periodo para los temas motor. En la Subfigura 4.7(a) la red temática para el cluster *BLACKHOLE*. En la Subfigura 4.7(b) la red temática para el cluster VANET. En la Subfigura 4.7(c) la red temática para el cluster *IDS*.

(a) (b)

Figura 4.8: Redes temáticas del primer periodo para los temas básicos/transversales. En la Subfigura 4.8(a) la red temática para el cluster WIRELESS-AD-HOC-SENSOR-NETWORK. En la Subfigura 4.8(b) la red temática para el cluster ROUTING-PROTOCOL.

4.1.4 Análisis del periodo 2016 - 2020

Al igual que en subperiodo anterior, primero se muestran los diagramas estratégicos para la cuenta de documentos (Subfigura 4.9(a)) e índice-h (Subfigura 4.9(b)) por temática.



(a) (b)

Figura 4.9: Diagramas estratégicos del segundo subperiodo (2016 - 2020). En la Subfigura 4.9(a) se ve el diagrama estratégico correspondiente al conteo de documentos, mientras que en la Subfigura 4.9(b) se observa el equivalente para el índice-h.

En los diagramas de la Figura 4.9, y las medidas mostradas en la Tabla 4.4 se aprecia como VANET se ha colocado en una posición de centralidad absoluta[3] en los últimos 5 años. MANET (como se verá mejor en su red temática 4.10(c)) ahora sí ocupa el centro de su cluster, y ambas temáticas se postulan como temas motor. Aparece en este periodo un nuevo tema motor PHYSICAL-LAYER-SECURITY, con un número de documentos pequeño, pero con un promedio de citas relativamente alto. Esto hace pensar que hay una nueva tendencia para asegurar la capa física.

En este periodo se observa que WIRELESS-AD-HOC-SENSOR-NETWORK se posiciona como temática transversal. Al igual que TRUST-MANAGEMENT, que se muestra como una evolución de la temática ROUTING-PROTOCOL del periodo anterior. Ambos temas reciben aún un número apreciable de citas. ASYMMETRIC-CRYPTOGRAPHY ha trasladado su posición a una zona más transversal, lo que indica que se ha usado más esta técnica en redes *Ad hoc* en los últimos años. Sin embargo, y aunque el número de documentos se ha duplicado, sigue siendo escaso para esta temática. El Índice-h tampoco ha crecido.

PRIVACY-PRESERVATION englobada en el periodo anterior en el cluster de VANET, se sitúa ahora de manera individual en el cuarto cuadrante, (ver Figura 4.9). Esta es la zona de temas poco desarrollados, bien por ser obsoletos o nuevos. Teniendo en cuenta que ya existía y que ha tomado relevancia para formar un cluster propio en este periodo, consideramos que se viene usando más, dando soporte a más tecnologías.

[3]Recordemos que la centralidad la marca el eje horizontal, una temática que se sitúe a la derecha del diagrama obtendrá toda la centralidad, sin importar la posición vertical que corresponde a la densidad.

Tabla 4.4: Medidas de rendimiento de los grupos del periodo 2016 - 2020.

Nombre del tema	Número de documentos	Índice-h	Promedio de citas	Número de citas
VANET	891	35	5,85	5.212
MANET	764	19	3,27	2.496
WIRELESS-AD-HOC SENSOR-NETWORK	246	18	5,91	1.455
TRUST-MANAGEMENT	194	16	4,76	924
SOFTWARE-DEFINED NETWORK-(SDN)	127	14	8,72	1.107
PRIVACY-PRESERVATION	101	14	6,85	692
ASYMMETRIC-CRYPTOGRAPHY	139	11	3,4	473
PHYSICAL-LAYER-SECURITY	61	10	8,69	530
UNMANNED-AERIAL VEHICLE-(UAV)	38	10	17,45	663
CLOUD-COMPUTING	53	9	7,25	384

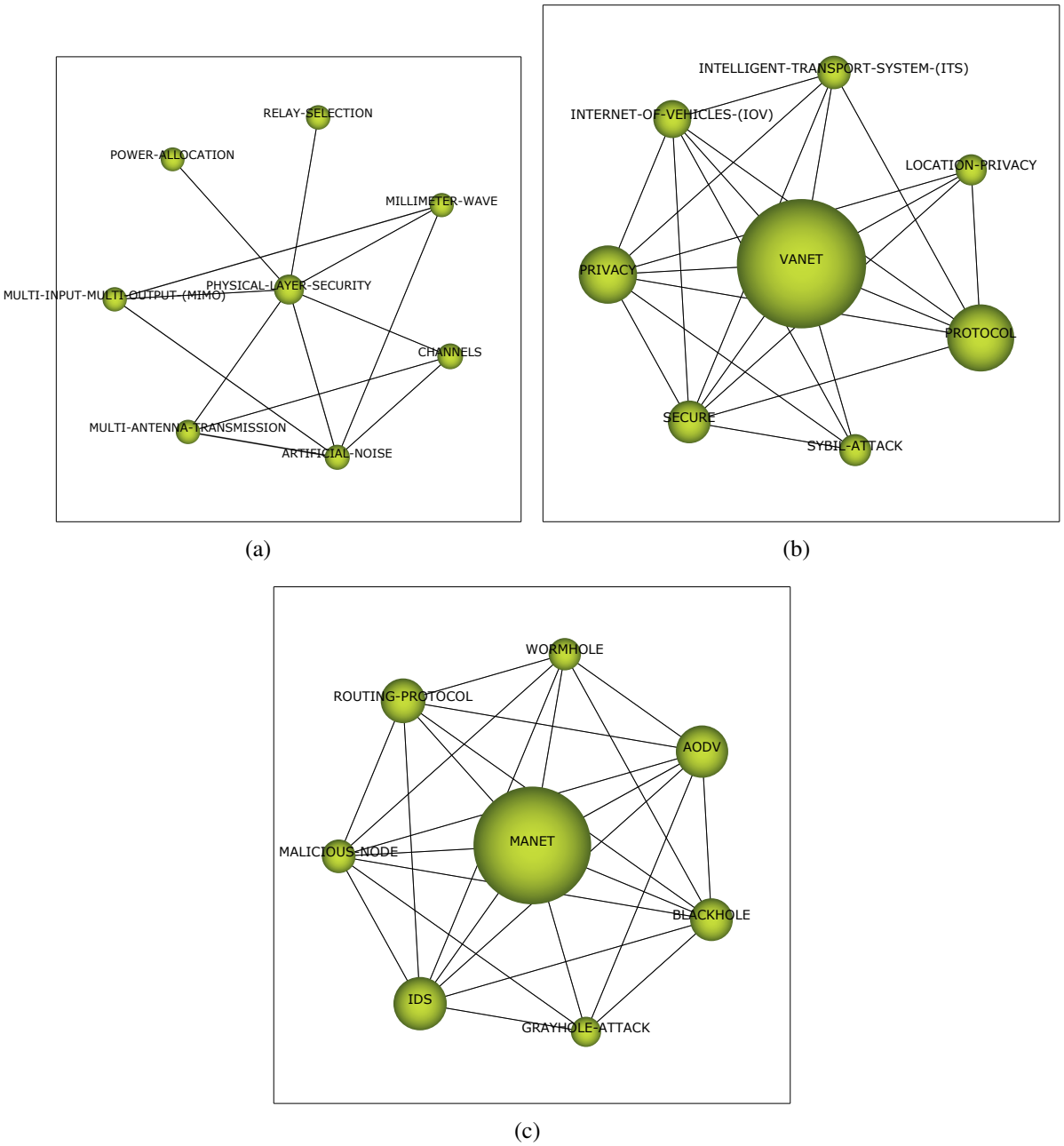
Por último, las temáticas UNMANNED-AERIAL-VEHICLE-(UAV), SOFTWARE-DEFINED-NETWORK-(SDN) y CLOUD-COMPUTING, de nueva generación, se posicionan en la zona de las temáticas especializadas emergentes. La temática de UAV con un número bajo de documentos ha alcanzado el mayor promedio de citas en su periodo.

En las Subfiguras 4.10(a), 4.10(b) y 4.10(c) se observan las redes temáticas para los temas motor en estos años. Como se comentaba, PHYSICAL-LAYER-SECURITY ha aparecido como una nueva temática motor, parece ser que ingenieros e investigadores tratan de hacer más segura esta capa.

En el cluster se incluyen temas de la capa física para la mejora de la seguridad. Entre ellos destaca el tema MILLIMETER-WAVE, que hace referencia a la tecnología de longitudes de onda extremadamente altas, (Extremely High Frequency (EHF)). La nueva tecnología de comunicaciones inalámbricas, que esta siendo usada para la nueva generación de comunicaciones móviles 5G. Por esta razón aparece dicho tema en estos años con esa presencia tan marcada.

La temática VANET sigue ocupando su posición de tema motor, con protocolos enfocados en la seguridad y la privacidad de la localización entre otros parámetros. Esta temática deja entrever como se está trabajando en la comunicación entre vehículos y su entorno, en lo que se ha empezado a llamar el INTERNET-OF-VEHICLES-(IOV). También se puede ver que aparece el SYBIL-ATTACK como posible punto débil afectando a la privacidad de los vehículos conectados.

El último tema motor es MANET. MANET sigue teniendo su propio punto débil, el *Packet Dropping*, afectando a su principal protocolo de routing AODV. Otro detalle de este cluster es que integra a IDS, esta temática del periodo anterior ha sido absorbida aquí, lo que hace pensar en que se está dedicando el uso de detección de intrusos de forma más intensa en MANET.



(a) (b)

(c)

Figura 4.10: Redes temáticas del segundo periodo para los temas motor. En la Subfigura 4.10(a) la red temática para el cluster PHYSICAL-LAYER-SECURITY. En la Subfigura 4.10(b) la red temática para el cluster VANET. En la Subfigura 4.10(c) la red temática para el cluster MANET.

En las Subfiguras 4.11(a), 4.11(b) y 4.11(c) se pueden ver los temas básicos/transversales del segundo periodo. En ellas se observa que WIRELESS-AD-HOC-SENSOR-NETWORK se ha posicionado como tema básico principal. Se puede observar que se sigue relacionando con muchos temas que no se relacionan entre si. Se trata de la temática básica de la que parten la gran mayoría de las investigaciones. De los subtemas detectados en esta red temática transversal, se deben destacar dos. INTERNET-OF-THINGS-(IOT), definición comercial del concepto de *interconexiones de dispositivos electrónicos cotidianos*, que puede o no basarse en redes *Ad hoc*. Y CYBER-PHYSICAL-SYSTEM-(CPS), un sistema ciberfísico (Cyber-Physical System (CPS)), según el Dr. Edward A. Lee [38], son integraciones de computación y procesos físicos. En el caso que ocupa este informe, se esta haciendo referencia a los vehículos autónomos en el contexto de VANET.

Por otro lado, las técnicas de *Trust Computing* han cogido relevancia en este periodo y forman su propio cluster, evolucionando desde ROUTING-PROTOCOL por las diferentes modificaciones de los distintos protocolos a nivel de capa de red. TRUST-MANAGEMENT es una temática transversal que se aplica en diferentes campos y técnicas de defensa.

Finalmente, ASYMMETRIC-CRYPTOGRAPHY se ha desplazado a la zona intermedia entre temáticas básicas y temáticas poco desarrolladas. Este desplazamiento desde el cuadrante de temas especializados y con aumento de la centralidad, puede significar un cambio a temática transversal. La relación con PRIVACY-PRESERVING-AUTHENTICATION hace pensar en posibles usos en redes vehiculares para la preservación de la privacidad, recordemos que el ataque que parece estar afectando a VANET, no es otro que el desdoblamiento de identidades de un nodo atacante, *Sybil*.

La aparición de PRIVACY-PRESERVATION como nodo central de un cluster situado en el cuadrante de temas poco desarrollados en el diagrama estratégico, indica que ha tomado más relevancia apareciendo como nueva temática, usándose más y soportando más tecnologías.

Las últimas redes temáticas del segundo periodo son las correspondientes a los temas especializados. SOFTWARE-DEFINED-NETWORK-(SDN) aparece como nueva temática en estos años. La configuración de redes definidas por software tienen la intención de facilitar la implementación e implantación de servicios de red de una manera determinista, dinámica y escalable, evitando al administrador de red gestionar dichos servicios a bajo nivel. Es un tema muy de actualidad y este hecho se observa en el considerable promedio de citas (Tabla 4.4).

UNMANNED-AERIAL-VEHICLE-(UAV), o redes de vehículos aéreos no tripulados. Esta temática ha recibido casi el doble de citas promedio que la más citada en este periodo, lo que pone de manifiesto su importancia para la investigación.

CLOUD-COMPUTING alcanza un promedio de citas parecido al de las Software Defined Networks (SDN). Aunque escasa en contenido, se puede destacar su relación con el tema VEHICULAR-CLOUD-COMPUTING-(VCC), de nuevo se pone sobre la mesa el estudio de tecnologías para las redes vehiculares.

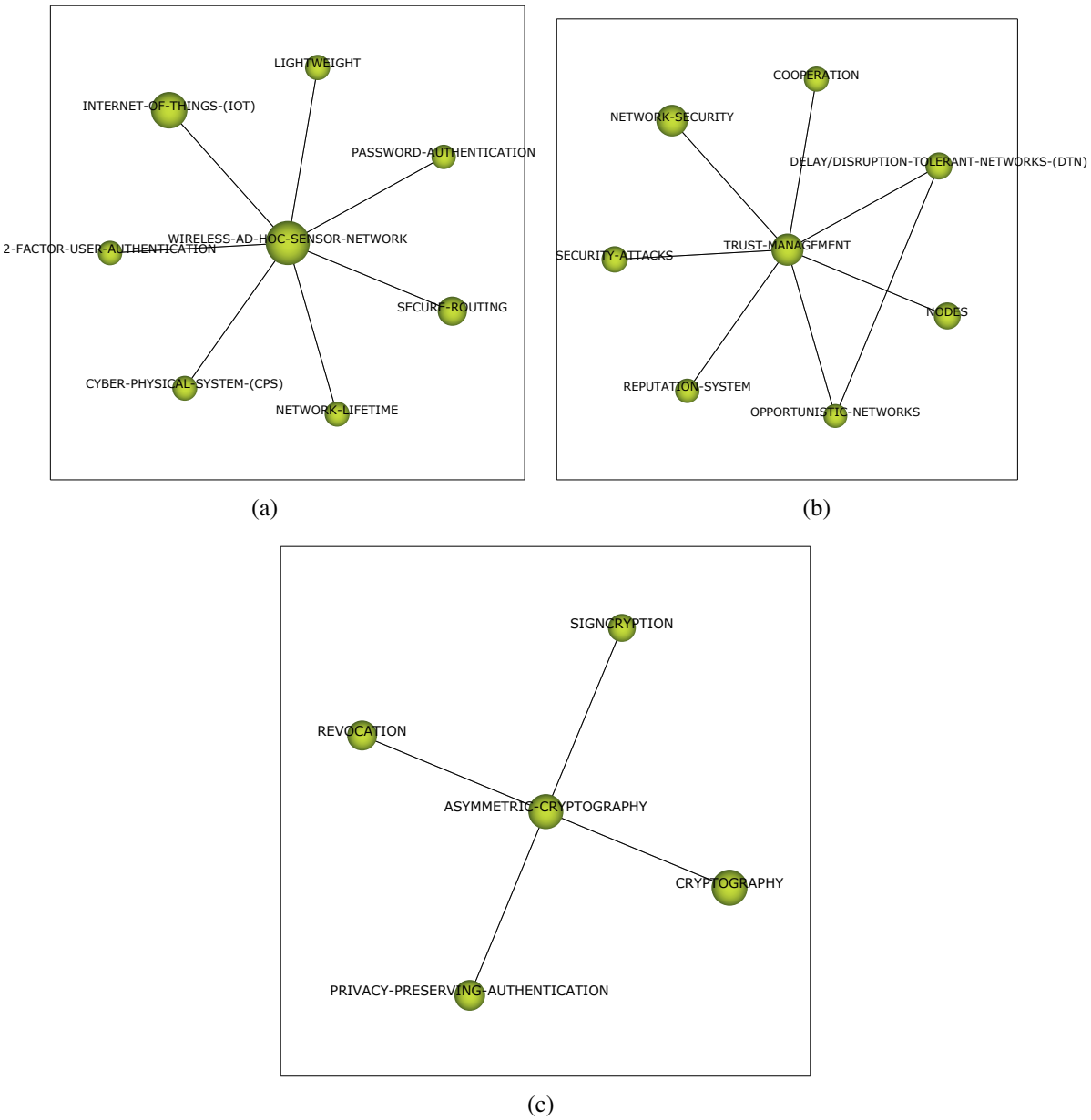


Figura 4.11: Redes temáticas del segundo periodo para los temas básicos/transversales. En la Subfigura 4.11(a) la red temática para el cluster WIRELESS-AD-HOC-SENSOR-NETWORK. En la Subfigura 4.11(b) la red temática para el cluster TRUST-MANAGEMENT. En la Subfigura 4.11(c) la red temática para el cluster ASYMMETRIC-CRYPTOGRAPHY.

4.1.5 Evolución y análisis longitudinal

Una vez extraídas y analizadas las distintas *Áreas Temáticas* en cada periodo y en cada cuadrante del diagrama estratégico, a continuación pasamos a analizar la evolución del número de palabras clave y el número de palabras clave compartidas en los diferentes subperiodos. Como se puede apreciar, las palabras clave de cada subperiodo pueden cambiar, ya sea en forma (léxico) o en número. El grupo de palabras clave evoluciona a través del periodo de tiempo para describir el contenido de los documentos. Aparecen nuevos temas con sus palabras clave asociadas y otros desaparecen. Pero también hay un subconjunto de palabras clave que se han mantenido sin cambios.

En la Figura 4.12 se muestra la evolución de las palabras clave. Los círculos representan cada subperiodo, y el número de palabras clave del subperiodo se representa en su interior. La flecha entre periodos representan el número de palabras clave compartidas entre ellas y, entre paréntesis, se muestra el Índice de Estabilidad[4] (fracción de superposición). La flecha que sale del primer subperiodo hacia arriba representa las palabras clave que no están presentes en el siguiente subperiodo. La flecha que entra en el segundo subperiodo desde arriba representa el número de palabras clave nuevas del subperiodo.

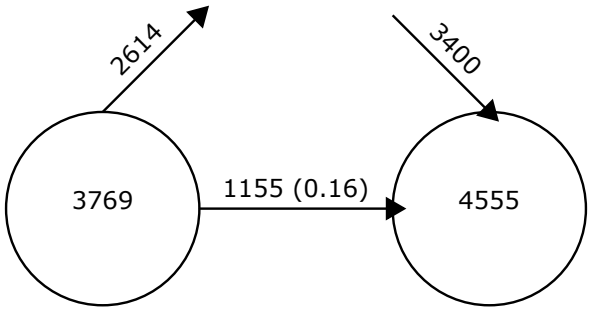


Figura 4.12: Diagrama de evolución de palabras clave para ambos subperiodos.

En el primer subperiodo (2011 - 2015) se puede observar que hay 3769 palabras clave, de las cuales 1155 permanecen en el siguiente subperiodo (2016 - 2020), con un índice de estabilidad de 0, 16. El resto de palabras clave, 2614, no siguen en el proceso, o son discontinuadas, mientras que para el siguiente subperiodo se incorporan 3400 nuevas palabras clave, sumando un total (junto a las que permanecen) de 4555. Como se podía esperar, en un campo de continua investigación y cambio, y avances tan rápidos, difícilmente se mantiene constante la terminología usada para definir el estudio. En general, en la ingeniería de la computación, el avance de la técnica es tan vertiginoso y cambiante que prácticamente aparecen nuevas tecnologías y conceptos cada año.

Una vez que se ha analizado la evolución de las palabras clave, pasamos a ver la evolución del caso de estudio a través de las *Áreas Temáticas*. Recordando la explicación de la sección 3.1 (ver Figura 3.4): *las líneas continuas significan que los temas vinculados comparten el nombre: ambos temas tienen el mismo nombre, o el nombre de uno de los temas es parte del otro tema. Una línea de puntos significa que los temas comparten elementos que no son el nombre del tema. El grosor de las líneas es proporcional al índice de inclusión, y el volumen de las esferas es proporcional al número de documentos publicados de cada tema.* En la Figura 4.13 se observa el mapa de evolución de las temáticas que se han detectado en el campo de la seguridad en redes

[4]Calculado entre 0 y 1

ad hoc. Se muestran las temáticas que han continuado sin cambios: VANET, WIRELESS-AD-HOC-SENSOR-NETWORK y ASYMMETRIC-CRYPTOGRAPHY; las que han continuado con algún cambio en el nombre: [(BLACKHOLE, IDS y WORMHOLE) ->MANET] y [ROUTING-PROTOCOL ->TRUST-MANAGEMENT]; y las que comparten elementos que no son el nombre de la temática [WIRELESS-AD-HOC-SENSOR-NETWORK ->TRUST-MANAGEMENT], [ROUTING-PROTOCOL ->WIRELESS-AD-HOC-SENSOR-NETWORK] y [WORMHOLE ->ASYMMETRIC-CRYPTOGRAPHY].

El mapa de evolución es algo denso por las interconexiones, sin embargo, si se detectan las diferentes *Áreas Temáticas*. En la misma Figura 4.13, se pueden observar sombreadas en diferente color los temas que compondrían cada una de esas *Áreas Temáticas* detectadas. Hay temas que tienen más de una sombra, lo que implica que el tema pertenece a más de un área temática. Por otro lado, hay temas que no tienen sombra, lo que implica que estos temas no pertenecen a ningún área temática.

Resumiendo, MANET encaja como un tema con una trayectoria dilatada. La investigación se ha volcado en asegurar los protocolos que se encargan de su funcionamiento, así se engloba ROUTING-PROTOCOL. Se ha puesto especial interés en contrarestar el *Packet Dropping* marcado como su principal punto débil, a la vista de como se recogen BLACKHOLE, GRAYHOLE-ATTACK y WORMHOLE, como subtemas dentro de MANET. Además, las técnicas de detección parecen haber sido la punta de lanza de las defensas para estas redes.

VANET es un tema intensamente estudiado en el ámbito de las redes vehiculares *Vehicle to vehicle* (V2V), *Vehicle to infrastructure* (V2I), y V2X en general. No quiere decir esto que las futuras redes de vehículos autónomos vayan a desarrollarse como redes vehiculares *ad hoc*, pero si están en el punto de mira como caso de estudio. La industria automovilística tiene totalmente claro que el salto revolucionario de generación de los automóviles pasa por la conducción autónoma del vehículo. Siendo como es un tema que dependerá de la minimización de fallos (los gobiernos no van a permitir el mínimo error en las carreteras), el I+D (o Research and development (R+D) en inglés) va a estar en continua prueba de tecnologías, a fin de encontrar la mejor solución posible.

Mientras WIRELESS-AD-HOC-SENSOR-NETWORK se mantiene como temática básica soportando así la investigación desde cualquier punto de vista. Engloba subtemas de cualquier ambito, como generalización de la propia investigación sobre seguridad en redes *Ad hoc*.

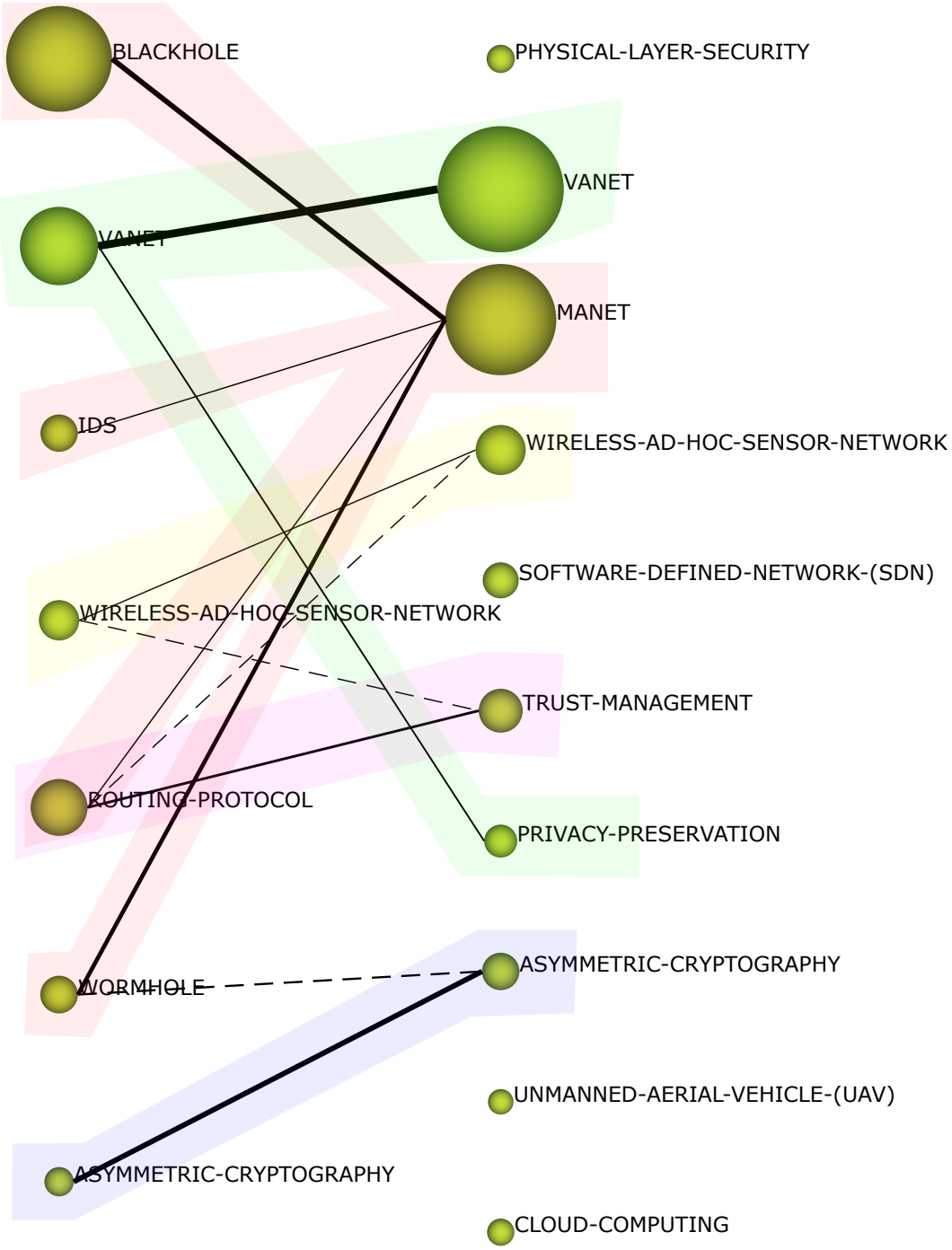


Figura 4.13: Mapa de evolución de las temáticas detectadas.

4.2 Estado actual de la Literatura: revisión sistemática

Del estudio bibliométrico de la Literatura se han extraído las temáticas que rodean a la investigación en lo que respecta a la seguridad en redes *Ad hoc*. Ha Quedado patente que actualmente es un tema que atrae la atención de la comunidad investigadora, sobre todo en MANET y VANET, temáticas en la que nos centraremos para realizar la revisión sistemática. Se empezará por exponer y describir los estudios secundarios de los que se ha hablado en la Sección 3.2: *Survey*s o revisiones del estado del arte actuales.

4.2.1 Revisiones del estado del arte

A continuación se exponen los trabajos de revisión más relevantes que dan una visión global sobre la temática en cuestión en el marco de la seguridad en redes VANET y MANET.

En el estudio realizado por Karagiannis *et al.* [80] se expone el estado de arte en arquitecturas de comunicación y aplicaciones en VANET en diferentes continentes y países. Así mismo destaca las principales líneas futuras de aplicación y estudio en donde indican que mucho más trabajo ha de hacerse en la línea de sistemas de verificación y *trust* en la capa de aplicación para evitar ataques *Impersonation*, *Fabrication* o *Tampering*. Para ello diferencian entre soluciones proactivas y reactivas. Las primeras basadas en criptografía y/o sistemas *anti-tampering* mientras que las segundas se centran en la detección de anomalías mediante Anomaly-Based Intrusion Detection System (Anomaly-Based IDS) o Signature-Based Intrusion Detection System (Signature-Based IDS). En este contexto, los autores concluyen con la necesidad de introducir dichos sistemas también como parte integrada en los vehículos.

Una de las principales características de las VANET es su dinamismo debido a la entrada y salida continua de nodos en la red. Este hecho hace difícil su autenticación e identificación, convirtiéndose en una de sus principales debilidades. Los autores en [52] hacen una revisión de soluciones basadas en la evaluación de la confianza entre nodos (*trust*) para mitigar los efectos de nodos maliciosos. Clasifican dichas soluciones basadas en infraestructura o no, aunque no mencionan como dichas soluciones mitigan los efectos de los atacantes ni que tipo de atacantes son. Con similar objetivo, el trabajo [70] presenta un estudio sistemático de la Literatura sobre soluciones *trust* en VANET. Los autores agrupan las soluciones en función del elemento en el que se quiere confiar distinguiendo entre: *entity-centric*, *data-centric* y *combined*. Además, proponen los requerimientos que todo sistema *trust* debería cumplir como por ejemplo sobre complejidad, escalabilidad o dinamismo, entre otros aspectos clave a cumplir en escenario VANET y que ninguna de las soluciones existentes contempla en su totalidad. Finalmente proponen una solución *trust* teórica basada en técnicas *Fuzzy Logic*. Sin embargo, no se habla del impacto y la viabilidad práctica de estos sistemas ante diferentes tipologías de ataques y amenazas, aspecto que se debería tener en cuenta en escenarios críticos como son las VANET.

Un trabajo de recopilación sobre problemas y amenazas a la seguridad en redes VANET se presenta en [75] prestando especial interés en la necesidad de soluciones que garanticen la fiabilidad y confianza (*trust*) en entre nodos. Son las especiales características de este tipo de redes las que que provocan sus principales debilidades en lo que respecta a la seguridad. Así, lo autores destacan como principales amenazas aquellas basadas en la modificación intencionada de mensajes (p. ej., *alteration* o *bogus information*) o aquellos que afectan a la disponibilidad del

sistema (p. ej., *Blackhole* o *message suppresion*). Los autores abogan por el uso de soluciones *trust* y además añaden nuevas características que dichos sistemas deberían contemplar de acuerdo a las únicas características de este tipos de redes. Algunas de estas son: escalabilidad, descentralización, robustez del propio sistema de *trust* y privacidad.

Otro trabajo recopilatorio sobre soluciones *trust* en VANET es propuesto en [32]. Los autores introducen los principales servicios de seguridad que se ven amenazados en este tipo de redes así como aquellas amenazas o ataques especialmente dirigidos a sus principales aplicaciones diferenciando entre *safety*, *secure communications* e *infotainment*. Sin embargo la contribución principal del trabajo es la clasificación de soluciones *trust* en función del ataque o ataques a los que hacen frente. Así, los autores diferencian entre soluciones contra ataques que *reenvían, alteran* y/o *injectan* mensajes no autorizados en la red; ataques específicos como el de *Blackhole*; ataques DoS y *Jamming*; ataques *fake location* o *timming*; y otros. Los autores concluyen la necesidad de soluciones adaptativas frente ataques que varían su comportamiento a lo largo del tiempo a los que denominan *smart attacks* y Advanced Persistent Threat (APT), así como la validación de las soluciones en entornos reales, principalmente debido a las especiales características de este tipo de redes que pueden limitar su aplicación práctica. Prácticamente todas las soluciones están orientadas a la detección de los anteriores ataques a través de la evaluación de niveles de confianza o reputación del nodo o información transmitida y responden a ello mediante el descarte del mensaje o el aislamiento del nodo.

Saif Sultan *et al.* [1] presentan un amplio resumen sobre tecnologías y aplicaciones en redes VANET. Los autores también indican retos relevantes a abordar en el futuro, entre los que se encuentra la seguridad y la privacidad. De acuerdo a los autores y en el contexto de la seguridad, estos apuntan a la necesidad de mantener la privacidad dentro de la provisión de sistemas *trust* en comunicaciones.

Los autores en [84] analizan el estado del arte en investigación en VANET identificando cuatro grandes temas: *routing*, *broadcasting*, Quality of Service (QoS) y *security*. En relación al último de ellos, identifican amenazas y ataques que afectan a este tipo de redes y comprometen diversos servicios esenciales de seguridad como son la confidencialidad (p. ej., *Eavesdropping*), disponibilidad (p. ej., DoS o *Blackhole*) y autenticación de nodos (p. ej., *Spoofing* variados o *Tampering*). Además, exponen diferentes soluciones y retos futuros de cada temática, destacando la provisión de soluciones criptográficas escalables y ligeras que eviten aproximaciones tradicionales basadas en criptografía asimétrica.

De forma similar al trabajo anterior, en [44] se introduce el concepto de VANET así como las tecnologías que las rodean y su clara aplicación en el contexto de los Sistemas Inteligentes de Transporte (ITS). En el contexto de la seguridad los autores exponen las principales amenazas a las que están sometidas este tipo de redes y a que servicios de seguridad afectan. Finalmente, se centran en aquellas soluciones basadas en criptografía que mitigan algunos de los principales ataques en este tipo de redes.

Sardana *et al.* [62], realizan una revisión de los aspectos fundamentales acerca de los protocolos de comunicaciones existentes en la Literatura, con un acercamiento a las definiciones que hace la Internet Engineering Task Force (IETF) sobre dos de los más relevantes en redes

MANET. Estos son: AODV[5] y Dynamic Source Routing (DSR)[6]. Además, los autores recopilan y caracterizan los principales ataques en redes MANET centrándose en el ataque *Blackhole*. Así diferencian entre ataques: (i) pasivos, (ii) activos, (iii) externos e (iv) internos. Terminan el artículo con una experimentación sobre como afecta el ataque *Blackhole* al protocolo AODV. Sin embargo, no aportan ninguna solución de defensa ante este tipo de ataques, aunque si concluyen la necesidad de aportar soluciones para hacerlo.

En [64], Saxena *et al.* estudian las técnicas de IDS y comentan la clasificación genérica por firmas, especificaciones o anomalías. Los autores no centran su estudio en una tipología de ataque concreto. De hecho, tratan de hacer trascender la importancia del IDS como primera capa de defensa para este tipo de redes. Para Saxena *et al.* los métodos preventivos clásicos basados en criptografía no son suficientes para *"evitar o eliminar"* los ataques, pasando IDS a tener un papel importante para la seguridad en MANET.

En [34] se estudia y analiza el estado del arte en soluciones de detección de ataques *Blackhole* y *Grayhole* en MANET. En dicho trabajo se diferencia entre soluciones IDS basadas en *clustering*, aquellas basadas en cooperación entre nodos, *Multilayer*, soluciones *trust*, etc., estas últimas difícil de enmarcar dentro de una línea de defensa concreta. Los autores concluyen la necesidad de soluciones distribuidas en donde los nodos cooperen entre sí, dinámicas y livianas entre otras, haciendo hincapié en la falta de soluciones que incluyan la notificación del ataque y su difusión efectiva, así como también soluciones enfocadas a mitigar ataques *Blackhole* o *Grayhole* colaborativos.

Los autores en [21] evidencian la falta de soluciones completas y arquitecturas de seguridad en redes VANET que contemplen la mayoría de las amenazas y ataques a los que están expuestos este tipo de redes. En el trabajo se introduce los principales requisitos de seguridad para el aseguramiento de redes y servicios en VANET como, por ejemplo, la autenticación, integridad, confidencialidad o privacidad, entre otros. Además presentan los principales ataques que atentan directamente contra los anteriores requisitos, sus características y perfiles, diferenciando entre ataques internos o externos, naturaleza, impacto, ámbito, etc. Con todo esto los autores proponen de forma teórica una arquitectura de seguridad basada en niveles y que comprende diferentes líneas de defensa.

Ghosal y Conti presentan en [24] un estudio muy completo de las características, las aplicaciones, así como de todos los retos que plantean este tipo de redes, además de los principales proyectos de investigación que se han llevado a cabo en el campo de las VANET. Clasifican los ataques en: 1) basado en patrones de comportamiento; 2) ataques al SW/HW; 3) ataques a la infraestructura; 4) ataques a la privacidad; y 5) ataques a la confianza de los datos. Además, clasifica y presenta las técnicas de defensa más relevantes en las que se está trabajando para solventar dichos ataques. Esta clasificación es: 1) criptografía de llave simétrica; 2) conservación de la privacidad; y 3) autenticación de mensajes.

Una revisión de diferentes estrategias basadas en el comportamiento del sistema inmune humano (*Artificial immune system* (AIS)), aplicadas a redes MANET se encuentra en el trabajo de Jim *et al.* [30]. Aquí se examinan con detenimiento las principales soluciones en las cuales se ha centrado la investigación sobre los algoritmos AIS, que son: (i) Algoritmo de Selección

[5] Ad hoc On-Demand Distance Vector
[6] Dynamic Source Routing

Negativa (Negative Selection Algorithm (NSA)), (ii) Redes Inmunes Artificiales, (iii) Algoritmo de Selección Clonal, (iv) Teoría del Peligro y (v) Algoritmos de Células Dendríticas. Los autores defienden una discusión entre ingenieros y biólogos, con el fin de enfocar el uso de estos mecanismos y buscar soluciones más robustas. Por ejemplo, en el caso de la detección de anomalías el algoritmo prepara un conjunto de ejemplo de detectores de patrones entrenados a partir de patrones normales (no-anómalos) que modelan y detectan patrones ocultos o anómalos.

Magán-Carrión *et al.* [42] también dedicaron sus esfuerzos en clasificar y describir ataques en redes *Ad hoc*, así como una revisión de técnicas que pudieran resultar tolerantes ante amenazas. Este trabajo se centra en ataques *Packet Dropping*, aunque menciona muchos más. Para los autores, es decisiva la búsqueda de soluciones que garanticen la continuidad de los servicios soportados por la red, y hacen una reflexión muy interesante al proponer la investigación de soluciones que actúen desde todas las líneas de defensa como un bloque único.

Korde *et al.* [37] realizan una reflexión sobre los puntos negros que debería cubrir una solución de seguridad enfocada a redes *Ad hoc* y más concretamente para MANET, como deben ser el suministro de energía, origen de la amenaza (externas o internas), cuántas capas de la pila de protocolos considera, etc. Sin embargo, auguran que ninguna técnica es capaz de dar solución a más de 2 ó 3 tipos de ataques. Los autores se refieren, en general, a la seguridad y supervivencia de MANET como el paradigma que persigue la investigación en este ámbito.

Mistry *et al.* [46] presentan las bondades del protocolo AODV para MANET tales como su dinamismo. A su vez hacen una revisión de varios trabajos relacionados con mitigar el ataque *Blackhole*, que aprovecha las debilidades de este protocolo. Según los autores, las defensas más exitosas vienen desde métodos basados en algún límite configurado para alguno de los parámetros relacionados con la red, como puede ser el conteo de mensajes Route REPly (RREP) o Route REQuest (RREQ), sobrepasado dicho límite, se tomarán las medidas oportunas. Esta técnica se conoce como umbral de "tolerancia".

Se ha repasado el estado de la Literatura para estudios similares, revisiones o *Survey*s, en la que se ha observado una falta de acuerdo en lo que respecta a la clasificación de las medidas de seguridad por líneas de defensa.

En la Tabla 4.5 se expone un resumen comparativo en relación a los trabajos anteriores. En dicha tabla, la columna "Ataques cubiertos" hace referencia a la tipología de ataque que cubre el trabajo (la generalización supone un enfoque más amplio). La columna "Clasificación" se refiere a si el artículo realiza alguna clasificación de las técnicas que revisa. La columna "Conclusión" hace referencia a alguna de las conclusiones más importantes extraídas del artículo. Las demás columnas son auto explicativas.

Tabla 4.5: Tabla resumen de Surveys.

Trabajo	Año	Ataques cubiertos	Clasificación	Conclusión
Karagiannis *et al.* [80]	2011	*Information attack*	Requisitos de VANET	Verificación y *Trust* como medidas más relevantes
Zeadally *et al.* [84]	2012	*Security threats*	Tipologías de ataques	Criptografía asimétrica escalable
Tangade *et al.* [75]	2013	*Modification & availability*	-	Garantizar la fiabilidad y la confianza
Al-Sultan *et al.* [1]	2014	-	Tecnologías y aplicación de VANET	Mantener la privacidad
Mejri *et al.* [44]	2014	Generalización	Tecnologías y aplicación de VANET	Criptografía
Engoulou *et al.* [21]	2014	Generalización	Requisitos de VANET	Arq. de seguridad por niveles con varias líneas de defensa (multicapa)
Patel *et al.* [52]	2015	-	Gestión de *trust*	Evaluación de la confianza
Soleymani *et al.* [70]	2015	-	Gestión de *trust*	Confianza por lógica difusa
Sardana *et al.* [62]	2015	*Packet Dropping*	Tipologías de ataques	Imprescindible la detección efectiva del *blackhole*
Kerrache *et al.* [32]	2016	*Security threats*	Gestión de *trust*	Evaluación de niveles de confianza
Jim *et al.* [30]	2016	Generalización	Algoritmos Bioinspirados	Algoritmos Genéticos de selección negativa los más apropiados para MANET

Tabla 4.5 continua de la página anterior

Trabajo	Año	Ataques cubiertos	Clasificación	Conclusión
Magán-Carrión *et al.* [42]	2016	*Packet Dropping*	Soluciones de resilientes	Desarrollar soluciones tolerantes
Korde *et al.* [37]	2017	Generalización	-	Se muestra interés en la supervivencia de la red
M. Mistry *et al.* [46]	2018	*Packet Dropping*	-	Desarrollo de soluciones con umbral de tolerancia
Saxena *et al.* [64]	2018	Generalización	Categorías de IDSs	IDS como 1ª línea de defensa.
Khanna *et al.* [34]	2019	*Packet Dropping*	Categorías de IDSs	Soluciones distribuidas. notificación y difusión
Ghosal *et al.* [24]	2020	Generalización	Tipologías de ataques. Y técnicas de defensa	La novedad del problema plantea múltiples líneas de investigación.

Figura 4.14: Gráfica del tipo de soluciones detectadas por los surveys revisados.

Como se observa en la Tabla 4.5, y la Figura 4.14, donde se muestra un recuento de tipos de soluciones detectadas en los *Survey*s anteriores. Se observa que siguen existiendo muchas propuestas de soluciones basada en sistemas de confianza y criptografía. Sin embargo, estas soluciones pertenecen a las revisiones de los primeros años expuestas en la tabla. Por otro lado, parece haber una nueva corriente de propuesta de soluciones tolerantes o resilientes[7], que conforman un paradigma nuevo de línea de defensa en la seguridad de redes *Ad hoc*.

[7]Según la RAE. Resiliencia: Capacidad de un material, mecanismo o sistema para recuperar su estado inicial cuando ha cesado la perturbación a la que había estado sometido.

4.2.2 Revisión Sistemática de la Literatura (*Systematic Literature Review*)

Como parte de la metodología de esta revisión sistemática, se plantearon las siguientes cuestiones de investigación:

Cuestión 4.1: ¿En que líneas de defensa se ha centrado la investigación en redes *Ad hoc*?

Cuestión 4.2: ¿Existe confusión en la clasificación por línea de defensa?

Cuestión 4.3: ¿Es necesaria la propuesta de nuevas taxonomías que añadan nuevas líneas de defensa?

Partiendo de las cuestiones anteriores, se plantea una búsqueda exhaustiva de documentos relacionados. Dicha búsqueda se realiza en diferentes bibliotecas digitales afines a las disciplinas tecnológicas, y en otras cuyo contenido es más general, y son consideradas referentes bibliográficos.

Como primer paso se establecen las palabras clave para la búsqueda de recursos, en lo que respecta a este trabajo. Una búsqueda general se realiza por *security "ad hoc"*[8], *Google Scholar*[9] muestra una cantidad de resultados muy grande, aproximadamente $2M$ de resultados. En cualquier campo relacionado con la Ingeniería de Computadores el tiempo es un factor a tener en cuenta, por lo que se acota la búsqueda por rango de años, desde el 2000 hasta la actualidad, bajando el número de resultados a $1,2M$. Para refinar aún más, se incorporan términos específicos de la lista de palabras relacionadas con la temática que se desea, como networks, MANET, VANET, attack, prevention, detection, response, las tres últimas keywords acorde con las tradicionales líneas de defensa. Los términos MANET y VANET se utilizan dada su relevancia obtenida del análisis bibliométrico. Haciendo uso de la búsqueda avanzada se pueden incorporar esos términos y excluir los que no nos interesen, filtrar por años, etc. En la Figura 4.15 se ve un ejemplo de búsqueda avanzada. Con lo que se consigue reducir el número de resultados a $52,7K$. Resumiendo, la primera búsqueda general en *Google Scholar* se establece así: *security networks attack OR MANET OR VANET OR prevention OR detection OR response "ad hoc"* desde el 2000 hasta la actualidad; ofreciendo $52,7K$ resultados aproximadamente.

Comando de búsqueda avanzada en Google Académico:

```
1    security networks attack "ad hoc" MANET OR VANET OR prevention
     OR detection OR response
```

Se puede apreciar la ingente cantidad de información existente incluso con una búsqueda avanzada y refinada. Se hace evidente la necesidad de afinar aún más. Otros factores que se imponen son ajustar el rango de años, seleccionar la base de datos de donde se extraiga la información o el número de citas del artículo. Seguidamente se refina la búsqueda principal en tres etapas, una por cada línea de defensa clásica, primero por *prevention*, luego por *detection* y finalmente por *response*, configurada como sigue a continuación. Será necesario repetir esta búsqueda cambiando la línea de defensa que sí entra en la búsqueda por alguna de las dos que

[8] Se pone *Ad hoc* entrecomillado para hacer ver al lector que deberá establecer este término como una palabra/frase exacta en las diferentes bases de datos.

[9] Google Scholar.

no ha entrado en la anterior, es decir, en cada búsqueda se incluye una línea de defensa y se excluyen las otras dos.

Comando de búsqueda avanzada por línea de defensa, prevention. En Google Académico:

```
security networks attack "ad hoc" prevention MANET OR VANET -detection
-response
```

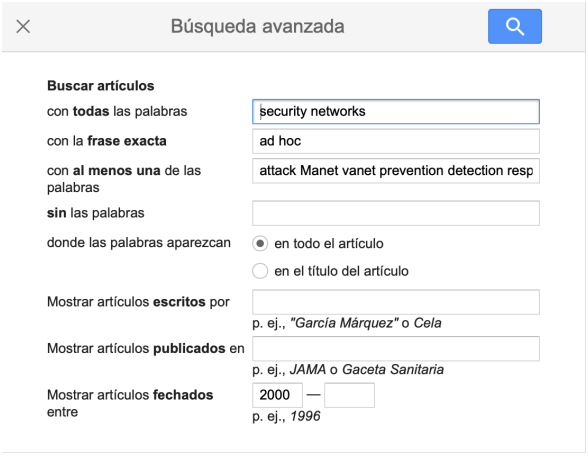


Figura 4.15: Ejemplo de búsqueda avanzada en *Google Scholar*.

A continuación se comentan las búsquedas realizadas en las distintas bibliotecas, para cada una se han configurado seis consultas equivalentes. La primera es una búsqueda general para *security "ad hoc"*. La segunda y tercera son reajustes por tipo de documento (artículos, libros, etc.) y área temática (ciencias de la computación), según la biblioteca permita estas configuraciones en las consultas. Las tres últimas son consultas especificas, configuradas para extraer los documentos relativos a una línea de defensa excluyendo las otras dos.

Se realiza una búsqueda siguiendo las pautas anteriores en la *Web of Science* del Ministerio de Ciencia, Innovación y Universidades. En primer lugar una búsqueda general para *security "ad hoc"*, como ya vimos en la Sección 4.1, pero esta vez con un rango de años desde el 2000, se obtienen aproximadamente $6,9K$ resultados. Seguidamente se hace una búsqueda amplia para las tres lineas de defensa juntas, se obtiene un resultado más afinado de alrededor de $1{,}7K$ documentos. Y una búsqueda específica para cada una de las tres líneas de defensa. En la Tabla 4.6 se muestra el resumen de búsqueda en WoS.

Tabla 4.6: Comandos de búsqueda usados y sus resultados en WoS (Mayo - Junio de 2020).

# Set	Query	Results
# 1	TEMA: (security AND "ad hoc")	$6,9K$
# 2	TS = (security "ad hoc") AND SU = (Engineering OR Computer Science)	$6,1K$
# 3	TS = (security networks "ad hoc") AND TS = (manet OR vanet OR prevention OR detection OR response) AND SU = (Engineering OR Computer Science) Refinado por: TIPOS DE DOCUMENTOS: (ARTICLE)	$1,1K$
# 4	TS = (security networks attack "ad hoc" response) AND TS = (manet OR VANET) NOT TS=(prevention detection) AND SU = (Engineering OR Computer Science)	30
# 5	TS = (security networks attack "ad hoc" detection) AND TS = (manet OR VANET) NOT TS=(prevention response) AND SU = (Engineering OR Computer Science)	389
# 6	TS = (security networks attack "ad hoc" prevention) AND TS = (manet OR VANET) NOT TS=(detection response) AND SU = (Engineering OR Computer Science)	91

A continuación, en la biblioteca digital de la *IEEE Xplore Digital Library*[10], se realiza una búsqueda similar. Primero una búsqueda general para *security "ad hoc"*, que ofrece $9,3K$ resultados. A partir de aquí se refina de la misma forma, búsqueda refinada general, y por líneas de defensa, limitando los resultados a *Journals*, *Magazines* y *Books*. Se obteniene una salida de 204 contribuciones en total. A esta última búsqueda se le aplican los operadores booleanos correspondientes para extraer los resultados de cada línea, excluyendo los de las demás, para contrastar la cantidad de resultados para cada una de las diferentes líneas de defensa. En la tabla 4.7 se muestra el resumen de la búsqueda en *IEEE*.

Tabla 4.7: Comandos de búsqueda usados y sus resultados en IEEE Xplore Digital Library (Mayo - Junio de 2020).

# Set	Query	Results
# 1	security "ad hoc"	9354
# 2	(("All Metadata":security networks attack "ad hoc") OR "All Metadata":vanet prevention detection response Manet)	1863
# 3	(("All Metadata":security networks attack "ad hoc") OR "All Metadata":vanet prevention detection response Manet) Refined By: Content Type: Journals Magazines Books	204
# 4	((("All Metadata":security networks attack "ad hoc" detection) OR "All Metadata":vanet manet) NOT "All Metadata":prevention response) Refined By: Content Type: Journals Magazines Books	145
# 5	((("All Metadata":security networks attack "ad hoc" response) OR "All Metadata":vanet manet) NOT "All Metadata":prevention detection) Refined By: Content Type: Journals Magazines Books	40
# 6	((("All Metadata":security networks attack "ad hoc" prevention) OR "All Metadata":vanet manet) NOT "All Metadata":detection response) Refined By: Content Type: Journals Magazines Books	37

[10] IEEE Xplore Digital Library.

Se continuó con el mismo tipo de búsqueda en *Scopus*[11]. Para la búsqueda general *security "ad hoc"*, la biblioteca ha ofrecido $13,6K$ resultados. Mientras que para la búsqueda filtrada por tipos de documentos a *Article*, *Book*, *Chapter* y *Review Book* se obtienen $1,7K$ resultados. Finalmente, se le aplican los filtros adecuados para extraer únicamente los documentos que correspondan a cada una de las líneas de defensa. En la Tabla 4.8 se muestra el resumen de la búsqueda en *Scopus*.

Tabla 4.8: Comandos de búsqueda usados y sus resultados en Scopus (Mayo - Junio de 2020).

# Set	Query	Results
# 5	TITLE-ABS-KEY (security "ad hoc") AND PUBYEAR >1999	$13,6K$
# 6	(TITLE-ABS-KEY(security AND networks AND attack "ad hoc") OR TITLE-ABS-KEY (vanet AND MANET AND prevention AND detection AND response)) AND PUBYEAR >1999 AND (LIMIT-TO (SUBJAREA, "COMP") OR LIMIT-TO (SUBJAREA, "ENGI"))	$4,7K$
# 7	(TITLE-ABS-KEY(security AND networks AND attack "ad hoc") OR TITLE-ABS-KEY (vanet AND MANET AND prevention AND detection AND response)) AND PUBYEAR >1999 AND (LIMIT-TO (SUBJAREA, "COMP") OR LIMIT-TO (SUBJAREA, "ENGI")) AND (LIMIT-TO (DOCTYPE, "ar") OR LIMIT-TO (DOCTYPE, "ch") OR LIMIT-TO (DOCTYPE, "re") OR LIMIT-TO (DOCTYPE, "bk"))	$1,7K$
# 8	(TITLE-ABS-KEY (security AND networks AND attack "ad hoc" prevention) OR TITLE-ABS-KEY (vanet AND manet) AND NOT TITLE-ABS-KEY (detection AND response) AND PUBYEAR >1999 AND (LIMIT-TO (DOCTYPE, "ar") OR LIMIT-TO (DOCTYPE, "ch") OR LIMIT-TO (DOCTYPE, "re") OR LIMIT-TO (DOCTYPE, "bk") AND (LIMIT-TO (SUBJAREA, "COMP") OR LIMIT-TO (SUBJAREA, "ENGI")	328

[11] Scopus.

Tabla 4.8 continua de la página anterior

# Set	Query	Results
# 9	(TITLE-ABS-KEY (security AND networks AND attack “ad hoc” detection) OR TITLE-ABS-KEY (vanet AND manet) AND NOT TITLE-ABS-KEY (prevention AND response) AND PUBYEAR >1999 AND (LIMIT-TO (DOCTYPE, “ar”) OR LIMIT-TO (DOCTYPE, “ch”) OR LIMIT-TO (DOCTYPE, “re”) OR LIMIT-TO (DOCTYPE, “bk”) AND (LIMIT-TO (SUBJAREA, “COMP”) OR LIMIT-TO (SUBJAREA, “ENGI”)	757
# 10	(TITLE-ABS-KEY (security AND networks AND attack “ad hoc” response) OR TITLE-ABS-KEY (vanet AND manet) AND NOT TITLE-ABS-KEY (prevention AND detection) AND PUBYEAR >1999 AND (LIMIT-TO (DOCTYPE, “ar”) OR LIMIT-TO (DOCTYPE, “ch”) OR LIMIT-TO (DOCTYPE, “re”) OR LIMIT-TO (DOCTYPE, “bk”) AND (LIMIT-TO (SUBJAREA, “COMP”) OR LIMIT-TO (SUBJAREA, “ENGI”)	264

En el caso de *ACM Digital Library*[12], las consultas mostradas en la Tabla 4.9 no sirven como retroalimentación y es necesario configurar la búsqueda nuevamente. Para la búsqueda general, la base de datos devuelve $32,1K$ resultados, siendo 517 revistas. De igual forma, se reduce la búsqueda para cada línea de defensa. En la tabla 4.9 se muestra el resumen de la búsqueda en *ACM*.

También se hace el mismo proceso en *Springer Link*[13] . De un modo parecido a *ACM Digital Library*, el comando de búsqueda no sirve como retroalimentación, es más, *Springer Link* ni siquiera guarda las búsquedas anteriores, así que el proceso es más manual. Por lo tanto, será necesario configurar una búsqueda completa para cada consulta. Para la búsqueda general para *security "ad hoc"*, la base de datos devuelve unos $56K$, mientras que para la búsqueda refinada y por tipo de documentos es de 820. Seguidamente se establecen los mismos filtros para las líneas de defensa. En la Tabla 4.10 se muestra el resumen de la búsqueda en *Springer Link*

Tabla 4.9: Comandos de búsqueda usados y sus resultados en ACM Digital Library (Mayo - Junio de 2020).

# Set	Query	Results
# 1	security AND "ad hoc"	$32,1K$
# 2	AllField:(security AND networks AND attack AND "ad hoc") AND AllField:(OR MANET OR VANET OR prevention OR detection OR response)	$9,97K$
# 3	AllField:(security AND networks AND attack AND "ad hoc") AND AllField:(OR MANET OR VANET OR prevention OR detection OR response) Filtering by Journal	517
# 4	AllField:(security AND networks AND attack AND "ad hoc" prevention) AND AllField:(OR MANET OR VANET) NOT AllField:(detection OR response) Filtering by Journal	22
# 5	AllField:(security AND networks AND attack AND "ad hoc" detection) AND AllField:(OR MANET OR VANET) NOT AllField:(prevention OR response) Filtering by Journal	39
# 6	AllField:(security AND networks AND attack AND "ad hoc" response) AND AllField:(OR MANET OR VANET) NOT AllField:(prevention OR detection) Filtering by Journal	18

Tras realizar esta serie de búsquedas en las diferentes bibliotecas digitales, se han extraído datos sobre el número de *papers* en cada caso, y se ha tratado de obtener una panorámica de como se ha enfocado la investigación. La Tabla 4.11 muestra un resumen de la información obtenida, donde se observa que una gran parte del esfuerzo se ha volcado en la detección.

[12] ACM Digital Library.
[13] Springer Link.

Tabla 4.10: Comandos de búsqueda usados y sus resultados en Springer Link (Mayo - Junio de 2020).

# Set	Query	Results
# 1	'security AND "ad hoc"' within 2000 - 2020	$55,9K$
# 2	'security AND networks AND attack AND "ad hoc" AND (manet OR VANET OR prevention OR detection OR response)'	$12,5K$
# 3	'security AND networks AND attack AND "ad hoc" AND (manet OR VANET OR prevention OR detection OR response)' within Computer Science filter Article filter 2000 - 2020	820
# 4	'security AND networks AND attack AND prevention AND "ad hoc" AND (manet OR VANET) AND NOT (detection AND response)' within Computer Science; filter Article; filter 2000 - 2020	14
# 5	'security AND networks AND attack AND detection AND "ad hoc" AND (manet OR VANET) AND NOT (prevention AND response)' within Computer Science; filter Article; filter 2000 - 2020	96
# 6	'security AND networks AND attack AND response AND "ad hoc" AND (manet OR VANET) AND NOT (prevention AND detection)' within Computer Science; filter Article; filter 2000 - 2020	77

Se debe tener en cuenta que se han realizado búsquedas especificas para cada línea de defensa, mostrándose resultados que contuvieren, por ejemplo, la palabra *detection* en los campos indexados. Para WoS, como se explica al principio de la sección 4.1, los campos son título, resumen y palabras clave (para la etiqueta TS seleccionada para las consultas hechas en este trabajo). Cabe la posibilidad de que en un documento que haya devuelto una consulta especifica para *detection*, se pueda encontrar la palabra *response* a lo largo del documento, explicando su posible herramienta de respuesta. En el caso de *Google Scholar* las consultas pueden realizarse sobre todo el artículo, como se puede ver en la Figura 4.15.

Los datos mostrados reflejan, primero la dificultad de separar completamente la clasificación de soluciones por línea de defensa tradicionales y segundo la necesidad de trabajos como

Tabla 4.11: Resumen de las búsquedas en las distintas bibliotecas.

	Total	Revistas	Prevention	Detection	Response
Google Scholar	$2M$	$52,7K$	$4,3K$	$10,2K$	$5,2K$
Springer	$55,9K$	820	14	96	77
ACM	$32,1K$	517	22	39	18
Scopus	$13,6K$	$1,7K$	328	757	264
IEEE	$9,3K$	204	37	145	40
WoS	$6,9K$	$1,1K$	91	389	30
% de trabajos			21 %	61 %	18 %

el presente, que realicen una meticulosa revisión de la Literatura para comprender toda esta problemática.

Los criterios de selección de estudios están destinados a identificar aquellos estudios primarios que proporcionan evidencia directa sobre la pregunta de investigación. En el caso del presente trabajo, se han usado las cuestiones de investigación tanto para la selección de estudios primarios como secundarios, dando lugar a la siguiente lista de documentos, que responden a las cuestiones de investigación 4.1, 4.2 y 4.3.

La selección/evaluación de estudios realizada, da como resultado los siguientes estudios secundarios: [80], [84], [75], [21], [44], [1], [52], [62], [70], [42], [32], [32], [30], [37], [64], [46], [34], [24]. Que ya se han comentado en la Sección 4.2.1.

Además de los siguientes trabajos primarios: [47], [72], [33], [49], [31], [71], [73], [9], [81], [17], [39], [3], [82], [4], [10], [48], [40], [45], [16], [61], [6], [63], [23], [33], [20], [50], [79], [74], [2]. Estos trabajos se comentan a continuación a través de su clasificación en la taxonomía presentada en este informe de investigación.

A continuación, se hace una reflexión acerca de como se estructuran en estos momentos las técnicas usadas por línea de defensa, la cual se pretende refinar para así establecer una taxonomía extendida para tratar de clasificar de una manera más realista respecto a la metodología usada. Con esta clasificación lo que se intenta es poner en discusión la falta de claridad al tratar de ubicar los distintos trabajos por líneas de defensa.

4.3 Taxonomía extendida por línea de defensa

Antes de desarrollar nuestra propuesta de taxonomía, se tendrá en cuenta el siguiente apartado definitorio para las líneas de defensa tal como se entienden tradicionalmente.

4.3.1 Líneas de defensa tradicionales

Existen diferentes maneras de clasificar las soluciones de seguridad para redes y sistemas de comunicaciones. Las soluciones destinadas a redes *Ad hoc* no son una excepción. Por ejemplo, como ya se ha visto anteriormente, aquellas que se centran en ataques específicos [84], [62], [24], por tipo de red [21], por línea de defensa [34], etc. En relación a las líneas de defensa, tradicionalmente podemos distinguir entre tres [22]:

- **Prevención.** En esta línea se agrupan los mecanismos de seguridad que tratan de prevenir ataques. En especial, aquellas soluciones que enfocan sus esfuerzos en preservar servicios de seguridad como la confidencialidad, la integridad, el no repudio y la disponibilidad de los servicios o cualquier elemento del sistema. Estos mecanismos defienden y protegen dicho sistema, evitando que el ataque llegue a producirse. Sobre todo, se basan en soluciones de autenticación y control de acceso, gestión de perfiles según los recursos a los que un usuario pueda o no acceder, criptografía, Intrusion Prevention System (IPS) y/o *Firewalls*.
- **Detección.** Son mecanismos de detección aquellos destinados a identificar actividades

inadecuadas, incorrectas o anómalas dentro de las redes o sistemas bajo monitorización. Destacar aquí los famosos IDS utilizados tanto en redes de comunicación (Network Intrusion Detection System (NIDS)) o en sistemas finales (Host Intrusion Detection System (HIDS)) [43]. Cuando un ataque es detectado, el proceso lógico sería actuar frente a dicha amenaza. En este punto es donde entra en juego la siguiente línea de defensa para responder ante el ataque detectado.

- **Respuesta.** Una vez detectado el ataque, el paso siguiente es responder ante dicha amenaza. Son soluciones que se agrupan en esta línea de defensa aquellas que se encargan, en cierto sentido, de paliar los efectos que tiene el ataque en curso. Esta respuesta estaría condicionada a la tipología y características del ataque en curso (ver Anexo A.1).

Magán-Carrión *et al.* [42] explican esta situación de una forma más extendida. En la Figura 4.16 se aprecia un esquema con una escala temporal. En dicho esquema se han tratado de representar de forma gráfica las comentadas líneas de defensa y dónde se enmarcan según el estado temporal concreto del ataque. Se observan dos líneas discontinuas que representan el momento justo de la detección de un ataque (entre los cuadrantes PREVENCIÓN y DETECCIÓN) y el momento de despliegue de las contramedidas (entre los cuadrantes DETECCIÓN y RESPUESTA). Con esta contextualización se pretende enmarcar a la prevención antes del ataque, a la detección durante el ataque (mientras se esté produciendo se detectará) y a la respuesta después de que se produzca el ataque y una vez detectado este. Sin embargo, en ocasiones encontramos soluciones que encajan muy cerca de los límites entre líneas de defensa, por lo que es común que los autores las clasifiquen en una u otra línea sin atender a estas directrices.

Además de las anteriores líneas de defensa tradicionales, aquí incluimos otra más: la tolerancia. Esta línea de defensa abarca todos los estadíos temporales de una ataque y no pretende a priori, mitigar los efectos del ataque si no tolerarlo. Como ya mencionaron Magán-Carrión *et al.* [42], haciendo referencia a la supervivencia[14] de la red. Soluciones tolerantes serían aquellas que abogan por preservar los servicios para los que se diseñó el sistema ante la presencia de ataques y principalmente evitan los tiempos, normalmente, largos entre la detección efectiva del ataque y la mitigación efectiva de este [54]. (Figura 4.16).

Con todo lo descrito hasta ahora se pretende hacer ver la necesidad de una novedosa clasificación por línea de defensa, que recoja de la forma más específica y exacta posible el funcionamiento de las soluciones de seguridad encontradas en la Literatura y que mejore la actual y tradicional clasificación.

Hasta ahora, se ha detectado que la clasificación atendiendo a las líneas de defensa tradicionales se vería como se muestra en el diagrama de Venn de la Subfigura 4.17(a). Existe claramente un solape entre la forma de clasificar las soluciones existentes.

Lo que se propone es un nuevo enfoque en función del estadío del ataque, para recategorizar y reordenar las soluciones encontradas y estructurar una nueva taxonomía por líneas de defensa. Siguiendo el diagrama conceptual de la Subfigura 4.17(b), donde se acepta un cierto solape entre detección y respuesta, parcela que vienen a cubrir las medidas de detección que también actúan frente a la amenaza. Pero lo que se separa claramente es la prevención, actuando únicamente antes del ataque. Sin embargo, la nueva propuesta de línea de defensa, tolerancia, sí estaría

[14] Según M. Lima *et al.* [41], un enfoque de supervivencia tiene como objetivo permitir que las redes cumplan correctamente sus funciones críticas incluso en presencia de ataques o intrusiones.

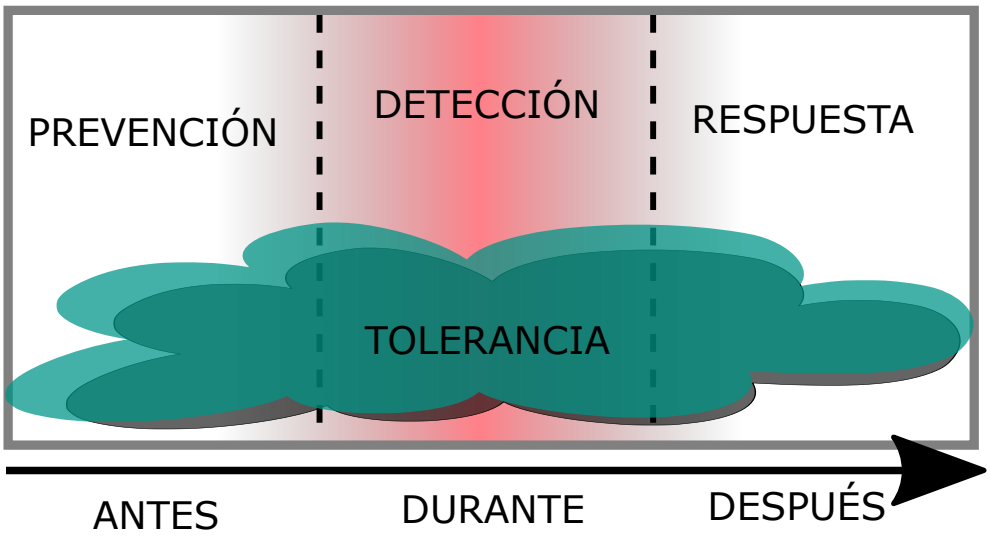
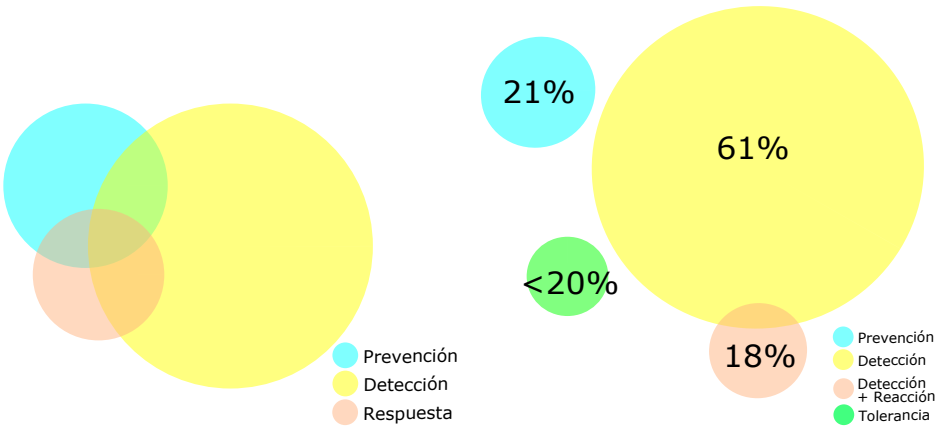


Figura 4.16: Esquema temporal de aplicación de líneas de defensa.

presente antes, durante y después del ataque. Los porcentajes presentados en la Subfigura 4.17(b) se corresponden con los de la Tabla 4.11 de la Página 88 para las líneas de defensas tradicionales. Se ha detectado que un pequeño porcentaje de los trabajos revisados podrían encajar como soluciones tolerantes.



(a) Líneas de defensa tradicionales (b) Propuesta del presente trabajo

Figura 4.17: Soluciones de seguridad en función de la línea de defensa implicada. En la Subfigura 4.17(a) se ve la agrupación según los autores. En la Subfigura 4.17(b) se ve nuestra propuesta de agrupación

A continuación, se propone una clasificación extendida para las líneas de defensa, atendiendo a su forma de actuar ante amenazas, y si esta actuación es previa al ataque (obstaculizándolo), o posterior a este (defendiéndolo).

Como se ha comentado antes (haciendo referencia a ese pequeño porcentaje de trabajos que encajarían como soluciones tolerantes (ver Subfigura 4.17(b))), existen mecanismos que no necesitarían de la detección, puesto que su estrategia de defensa consiste en tolerar los efectos negativos del ataque a parámetros de rendimiento del sistema. Sin embargo, tampoco serán soluciones de prevención porque no encajan en la definición clásica (ver página 89), ya que no tienen porque impedir el ataque. Además, su momento de actuación es pre y pos ataque. A estas

soluciones acordamos en llamarlas soluciones tolerantes. Por otro lado, vemos que las soluciones de reacción no tienen sentido sin una detección. Se propone entonces la siguiente taxonomía para líneas de defensas:

- **Prevención:** Aquellas soluciones que tratan de evitar el ataque, por lo que actúan antes del ataque. *Subsección 4.3.2*.
- **Detección:** Soluciones que detectan el ataque, por lo que actúan después del ataque, es decir, no lo evitan. Se clasifican las soluciones que realicen una detección pura, sin ninguna reacción en contra. *Subsección 4.3.3*.
- **Detección + Reacción:** Esta sección engloba aquellas soluciones que detectan el ataque y además realizan alguna labor de respuesta. *Subsección 4.3.4*.
- **Tolerancia:** Soluciones que no evitan el ataque, y en cuya acción se aprecia una intención por mitigar los efectos negativos que afecten a los servicios y rendimiento de la red. En lugar de realizar acciones de bloqueo. *Subsección 4.3.5*.

4.3.2 Prevención

Si se tiene en cuenta el sentido clásico de las soluciones preventivas, se debe hablar de técnicas criptográficas. Sin embargo, existen soluciones no criptográficas que encajarían como sistemas preventivos, ya que establecen algún tipo de medida cuya finalidad sea la de proteger la red evitando que se produzca el ataque. En esta subsección se clasifican los trabajos que han centrado sus esfuerzos en la prevención como núcleo de su enfoque de seguridad.

Con el trabajo realizado en [61], Sanzgiri *et al.* presentan el protocolo AuthenticatedRouting for Ad hoc Networks (ARAN) para combatir ataques *Sinkhole* ([56],[58]). ARAN asegura el enrutamiento en entornos MANET, para lo cual utiliza certificados criptográficos para realizar autenticación, integridad de mensajes y no repudio en el proceso de descubrimiento de ruta. Los autores comparan su solución frente a AODV, consiguiendo mejores resultados tanto en longitud media del camino como en carga de enrutamiento, al centrarse en la ruta asegurada, en lugar de la más corta. Además, consigue mejores resultados también para la Fracción de entrega de paquetes. El artículo asegura que las bondades de ARAN pasan por no utilizar parámetros como el conteo de saltos o el uso de rutas establecidas, si no en el uso de envío de mensajes firmados, que garantizan la autenticación de extremo a extremo.

En [16], los autores analizan los efectos de ataques *Blackhole* sobre una simulación de una red bajo AODV, midiendo el rendimiento antes y después del ataque, y además proponen una posible solución. A través de simulaciones de redes MANET, encontraron una posible clave en la velocidad de respuesta para los mensajes RREP, siendo el tiempo de llegada mayor para los que provenían de nodos honestos en comparación con los que emitían los nodos maliciosos. Basándose en sus resultados, implementaron Intrusion Detection System Ad hoc On-Demand Distance Vector (IDSAODV), un protocolo que prioriza la segunda ruta (segundo RREP recibido). Los resultados mostraron una mejora del 18 % en el Packet Delivery Ratio (PDR) en presencia de un agujero negro en la red, pero también notaron un ligero empeoramiento con respecto a la simulación en la que no había ningún ataque.

AntTrust [45] es un protocolo enfocado en dar seguridad al enrutamiento de redes Wireless Ad hoc NETworks (WANET) para contrarrestar ataques de tipo *Sybil*. *AntTrust* es un método

bio-inspirado basado en Ant Colony Optimization (ACO), que consta de tres agentes que realizan acciones separadas: 1) *Ant*: establecer rutas, 2) *Rectifier Ant*: detectar cambios en topología, 3) *Monitor Ant*: monitorizar comportamiento de los vecinos a un salto. *AntTrust* se testa con varios experimentos con diferente número de nodos y Time To Live (TTL), siendo capaz de elegir la ruta más corta. Los autores prueban que al configurar un nodo malicioso en esa ruta para un ataque *Sybil*, esa ruta comienza a perder confianza y la solución busca rutas alternativas.

Li *et al.* [40], con la idea de mejorar el PDR propone una mejora para AODV usando modelos de confianza a la que llamaron Ad hoc On-demand Trusted-path Distance Vector (AOTDV). Básicamente, cada nodo establece un nivel de confianza para sus vecinos según las respuestas sobre los paquetes que recibe y reenvía dicho nodo, siendo esta la confianza directa. Además, un nodo puede recomendar un vecino en el que tenga confianza, a esta la llaman confianza indirecta. Una vez se tienen estimaciones de confianza sobre un grupo de vecinos, el nodo fuente define una "ruta de confianza", o lo que los autores llaman una *trusted-path*. Según los autores, su protocolo mejora el PDR, y además mitiga los efectos de los ataques *Blackhole* A.2(b), *Grayhole* A.2(c) y *Modification* [83] A.6 (ver descripción en A.1).

Nabet *et al.* [48] presentan una actualización del algoritmo Secure Routing Protocol (SRP), al que han llamado Ad hoc Secure Routing Protocol (ASRP). SRP basa su funcionamiento en la autenticación y cifrado de extremo a extremo. Finalmente, los autores incorporan la filosofía de SRP al conocido AODV, añadiendo al protocolo los mensajes *KeyExchange* y *Authentication*. ASRP asegura el enrutamiento *Ad hoc*, pero no disuade comportamientos egoístas (o *selfish*). Los autores realizan una comparativa entre AODV y ASRP, donde declaran a este último más lento durante el descubrimiento de ruta, por la carga computacional que tienen las operaciones de autenticación.

En el trabajo [10] los autores basan sus esfuerzos en un algoritmo multicapa controlable por el usuario al que llaman *User-Controllable MultiLayer Secure Algorithm* (UMSA), con la idea de autenticar los nodos antes de que se unan a la red MANET. En UMSA la capa *Multilayer* es la encargada de calcular un código único que se incrusta al mensaje Mensaje *HELLO* del nodo para tratar de autenticarse con su vecino. Además, se añade una marca de tiempo para mantener sincronizada la red. Los autores realizaron una serie de experimentos, en los que algún nodo trataba de unirse a la red con unos parámetros preconfigurados, y comparando los resultados con los obtenidos de *Optimized Link State Routing* (OLSR)[15]. La seguridad, comentan sus autores, no se vio comprometida en el intento de autenticación del nodo correspondiente. Además, ni en retardo ni en ancho de banda se observa diferencia apreciable entre UMSA y OLSR.

En [4] Balakrishnan *et al.*, hacen referencia a los problemas derivados por ataques de denegación de servicio, concretamente en los ataques Null Frequency Jamming (NFJ), capaces de afectar de un modo drástico a las redes *Ad hoc*. Una contra medida eficaz para mitigar NFJ, según los autores, sería hacer aleatorios los periodos de recuperación de rutas a través de modelos matemáticos. Los autores presentan resultados en los que aseguran que su solución merma la aparición de NFJ. El proceso tiene un *handicap*, en la formulación matemática utilizan un límite para abarcar el rango de aleatorización, si dicho rango se hace demasiado grande, los tiempos de demora de la recuperación se alargan, por lo que tienen que calcular el límite máximo por debajo del cual estos tiempos sean aceptables.

[15] Optimized Link State Routing

4.3.3 Detección

Si hablamos de técnicas de detección, tenemos que nombrar las medidas IDS, cuya clasificación más general se divide en la detección basada en firmas y la detección basada en anomalías. Algunos ejemplos de estas últimas, muy comunes en entornos de redes *Ad hoc*, son aquellas basadas en sistemas de reputación en donde se establecen umbrales para determinar si un nodo es malicioso o no. En esta subsección vamos a clasificar los trabajos que han centrado sus esfuerzos en la detección como núcleo de su enfoque de seguridad.

En el trabajo [82], Ye *et al.* hacen uso de sistemas de detección de intrusos basados en Hide Markov Model (HMM), en entornos MANET. Se trata de un sistema de detección de anomalías. El sistema funciona por *clusters* de nodos, monitorizados por un nodo central o Cluster Head (CH), dicho nodo gestiona una cola de supervisión de mensajes de comportamiento del vecindario (su *cluster*). El modelo HMM detecta estados, siendo su salida binaria, 0 y 1 para los estados normal y anómalo respectivamente. Tras realizar una serie de experimentos en redes MANET para poner a prueba el modelo, utilizando AODV como protocolo de enrutamiento, los autores llegan a la conclusión de que su propuesta es capaz de detectar ataques, pero no de clasificarlos.

Baadache y Belmehdi proponen en [3] el uso de *Merkle tree* y funciones *hash* para contrarrestar ataques de *Packet Dropping*. Para comprobar el uso del sistema, simulan redes basadas tanto en AODV como en OLSR con la idea de abarcar los dos tipos de protocolos. La solución se basa en el cómputo de dos *Merkle tree*: uno en la fase de descubrimiento de ruta y otro en el proceso de comunicación. Si ambos valores coinciden significará que el siguiente salto ha recibido el paquete. Se realizaron experimentos en dos modelos: Total Acknowledgment (TA) y Random Acknowledgments (RA). Durante el experimento se consiguieron detectar los paquetes que eran descartados en los dos modelos, llegando a tener un éxito cercano al 100 % en TA, y de alrededor del 90 % en RA, que parece depender de los valores definidos para la probabilidad de éxito de los acuses de recibo.

Los autores en [39] plantean un IDS en VANET que se basa en la evaluación de la confianza *trust* en términos de a) la información transmitida o *data trust*, donde los autores evalúan cómo de confiable es la información que se transmite y b) en términos del funcionamiento del nodo en concreto o *node trust*, evaluando como este se comporta de acuerdo a como debería hacerlo. Para computar ambos parámetros los autores utilizan enfoques basados en la teoría de evidencias a través de la información recibida y predicción de la confianza en un nodo mediante la opinión de otros en la red. Los autores miden el rendimiento del sistema en simulación ante la presencia de nodos maliciosos de varios tipos a los que llaman: *simple attack* que afecta al propio protocolo de comunicación; *bad mouth attack* que produce información falsa; y *zigzag (on-and-off) attack* que mezcla ambos ataques y además es intermitente. La solución propuesta mejora con respecto al estado del arte, en términos de rendimiento de detección ante diferente porcentaje de nodos atacantes, diferentes velocidades y número de nodos en la red.

En la referencia [17], Dorri *et al.* propone un enfoque más al protocolo AODV, a través de un paquete de control adicional y una tabla de información de enrutamiento de datos extendida Extended Data Routing Information (EDRI). El autor asegura que su enfoque aumenta el número de nodos confiables, disminuye la sobrecarga y mejora el retraso de los paquetes, además de eliminar los falsos positivos. Se trata de extender la tabla Data Routing Information (DRI) con

un campo más, el cual se establecerá a 1 cuando se detecte un *Blackhole*, mientras no haya detección, este campo se mantiene a 0. Los autores comparan su técnica con la de Sen *et al.* [65], basada esta última en DRI y verificación cruzada. En los resultados mostrados, se aprecia una disminución de los paquetes RREQ necesitados, así como un descenso en el *Delay* de la red y un aumento del rendimiento.

Verma *et al.* [81] presentaron otro enfoque, llamado *New Fresh*, contra el ataque de agujero de gusano. Se trata de un algoritmo del cual aseguran detecta efectivamente el ataque *Wormhole*. La técnica compara la ruta seguida por un paquete con la que previamente estaba en la tabla de rutas del nodo fuente. Además, se realiza un cálculo de la tasa de paquetes enviados/recibidos para cada comunicación. Variaciones en la comparación de las rutas, o un valor de PDR menor que 1, denotarían la existencia de un *Packet Dropping* en cualquiera de sus formas. El algoritmo se puso a prueba en redes simuladas comparándolo con AODV, y se analizan la tasa de entrega de paquetes, el rendimiento y el *Delay* de extremo a extremo, mostrando resultados en los que se observa como la propuesta *New Fresh* vence al clásico AODV en todas las métricas.

Chourasia *et al.* [9] presentaron otra propuesta IDS para combatir *Packet Dropping*. Se trata de un algoritmo de conteo de saltos en dos tiempos. Uno en el descubrimiento de ruta, en la recepción del RREP el nodo fuente recibirá con él un valor equivalente al número de saltos. El segundo, más tarde al enviar la información, se cuentan los saltos que realiza el paquete, cuando llegue a destino se restan los dos valores, y el resultado debe dar 0, siendo así, se podrá decir que la ruta es segura y realmente la más corta al destino. Se realizan simulaciones con AODV como protocolo de enrutamiento y se obtienen datos con y sin su IDS en funcionamiento, mostrando unos resultados del rendimiento para el PDR del 98 %.

4.3.4 Detección + Reacción

Es usual encontrar en la Literatura soluciones basadas en IDS más complejos que son capaces de responder tras la detección. En esta subsección se recogen dichos sistemas.

Su *et al.* [73] y [71], proponen mitigar ataques de tipo *Blackhole* con la incorporación de elementos IDS, estableciendo una diferencia máxima entre mensajes RREQ y RREP, si un nodo excede dicho límite, los IDS emiten mensajes de bloqueo para que los nodos normales incluyan al sospechoso en sus listas negras. La configuración de los IDS la realiza un algoritmo al que llaman Anti-Black Hole Mechanism (ABM), basado en dos tablas. En una de ellas, la tabla Suspicius Node (SN) se apuntan las veces que un nodo concreto envía mensajes de RREP que no parecen razonables, mientras en la tabla Block Table (BT) se registran los nodos que han sido marcados como maliciosos. Los autores validan ABM en redes MANET, tratando de mitigar la acción de dos nodos *Blackhole* (primero fijos y luego en movimiento) frente al protocolo AODV, llegando a reducir la perdida de paquetes en una cantidad muy elevada.

En el trabajo [31], Katal *et al.*, estudian otro tipo de ataque, el Datagram Chunk Dropping como otra forma de *Packet Dropping* enfocado a redes MANET que transmiten datos multimedia. Los autores hablan en este artículo de la calidad del servicio (QoS) como objeto afectado, y ofrecen una técnica basada en *clusters* para detectar y prevenir este tipo de ataque. La llaman Cluster Based Datagram Chunk Dropping Detection and Prevention Technique (CBDCDDPT), la cual tiene como base un nodo "líder" (CH) elegido entre el grupo de nodos. El nodo CH

recibe un buffer desde el emisor/fuente, que contiene un número de secuencia y el trozo de dato correspondiente. Dicho buffer debe coincidir con el que también manejan los nodos intermedios de la ruta de emisión. Si el nodo observador detecta alguna incongruencia en el buffer (concretamente entre los números de secuencia) expulsa al nodo sospechoso de la red. Para comprobar la eficacia de su algoritmo, realizaron pruebas usando AODV como protocolo de enrutamiento y su propuesta para detectar los ataques. Los autores muestran los resultados en rendimiento del flujo de datos en *kbps* (kilo bits por segundo). Para el el escenario con ataque y sin respuesta el rendimiento fue del 96 %. Mientras que para el escenario con ataque y respuesta el rendimiento fue del 98 %. Mediciones en relación al escenario sin ataque.

Nadeem *et al.* [49] proponen un sistema con el que aseguran mejoras con baja sobrecarga de la red, y al que llaman Intrusion Detection & Adaptive Response (IDAR). Aseguran que es capaz de proteger una red MANET ante varios tipos de ataques, *Blackhole* entre otros. Este mecanismo responde en cuatro fases: (i) detección de intrusos, (ii) identificación del ataque, (iii) identificación de intrusos y (iv) respuesta de intrusión adaptativa. Los autores presentan una lista de castigos acorde a la acción detectada, desde el aislamiento hasta dejar sin castigo. Tras poner a prueba su propuesta trabajando con AODV, y simular ataques de tipo DoS, *Blackhole* (y derivados), y *rushing*, los autores muestran resultados del funcionamiento de su técnica. Lo curioso es que tanto para DoS como para *Blackhole*, IDAR decide aislar al atacante, mientras que para *rushing* no, siendo tolerante con un ataque que no parece ser tan dañino.

En [33] Khan *et al.* presentaron un sistema de detección y prevención en redes MANET, al que llamaron Detection and Prevention System (DPS). Los autores enfocaron sus esfuerzos en los ataques de agujeros de gusano, advirtiendo que el número de RREQ realizados por estos nodos era menor que el del resto de la red. Siguiendo esta pauta, configuraron un sistema con tres roles: (i) nodos normales, (ii) nodos maliciosos y (iii) nodos DPS. Estos últimos son los encargados de interpretar los estados y acciones de los nodos a su alcance (respuestas de RREQ detectadas), información que mantienen en una serie de tablas. Cuando un nodo DPS observa variaciones entre dos valores establecidos como *Min_Req_Count* y *Max_Req_Count* (mínimo y máximo recuento de RREQ para un mismo nodo) que dependen del comportamiento del vecindario, se inicia un proceso algorítmico que, a grandes rasgos, puede elevar el valor de sospecha sobre un nodo, o si este valor supera un umbral, se emitirá una alerta de amenaza, o de bloqueo según proceda. Los autores pusieron a prueba el sistema sobre simulaciones MANET, usando *Wormhole* fijos y móviles, con una disminución del PDR del 53 %-54 % tras usar su propuesta. También compararon resultados con la propuesta de Su *et al.* [72], mostrando una reducción del 93 %-98 % de la tasa de falsos positivos.

La propuesta de Muthurajkumar *et al.* [47], a la que han llamado Cluster based Energy Efficient Secure Routing Algorithm (CEESRA), también basada en clusters, y que trata de gestionar problemas de eficiencia energética, propone un algoritmo de enrutamiento con umbral de confianza, gestionado por los CH. En función del ratio entre Acknowledgement (ACK) enviados y paquetes recibidos, el sistema reacciona ignorando los posibles nodos maliciosos detectados a la hora de reformar los *clusters*. Los autores compararon su propuesta con AODV, así como con AOTDV (la propuesta de Li *et al.* [40] descrita en la página 93 de este documento). El factor clave de sus experimentos es la velocidad de los nodos, ya que los resultados van en decremento en cuanto aumenta la velocidad. Aun así, para la tasa de descarte de paquetes, se observa una reducción de entre un 80 % y un 50 %, y para el rendimiento, CEESRA supera a AOTDV en un 50 %.

En la referencia [2], Ansari *et al.* se centran en ataques DoS, concretamente en el conocido como *Flooding* (inundación), ataque que puede afectar a cualquier capa y que trata de agotar los recursos de los nodos MANET. Los autores aconsejan usar técnicas de capas cruzadas para detectarlos. Los autores hacen referencia al hecho de que este tipo de ataque es llevado a cabo por un nodo que trata de ahorrar su propia energía. Por lo tanto, estos ataques se realizan generando datos de baja potencia, con un alto Bit Error Rate (BER) y una baja Signal to Noise Ratio (SNR). El método va controlando las estadísticas de una serie de parámetros para todos los nodos (BER y SNR entre otros). Cuando se observa que alguno de esos parámetros varía más de un porcentaje preconfigurado en el algoritmo, se empieza marcando al nodo como sospechoso. Cuando el número de sospechas crece, se lanza un mensaje de *warning* al *clusters*/red. Si aun así el nodo sigue inundando, se introduce como registro en una lista negra. Los autores realizan simulaciones del proceso de ataque varias veces alternando la velocidad de transmisión de datos, y concluyen que una velocidad moderada mejora la precisión de detección para su propuesta.

Noguchi *et al.* [50], proponen un método dinámico de prevención de agujeros negros (*Blackhole*) que se base en el establecimiento de umbrales. Dichos umbrales se calculan a partir del número total de nodos activos y el tiempo transcurrido desde la recepción del último paquete de control de enrutamiento. Cada nodo verifica si el número de secuencia RREP recibido es mayor que dicho umbral. Cuando esto sucede, el origen del RREP se considera un *Blackhole* añadiéndolo a una lista negra que se mantiene en constante actualización. Cada cierto tiempo un nodo vuelve a juzgar a los integrantes de su lista negra, para lo cual, inunda la red con un falso RREQ de destino aleatorio, al que solo un nodo *Blackhole* respondería, de modo que aquel nodo que responda con un RREP al paquete trampa será añadido a la *black list* o, en caso de ya estar marcado, su tiempo de "castigo" se restablecerá. En comparación con Secure Route Discovery for the AODV protocol (SRD-AODV) [74], una evolución anterior de AODV también basada en umbral, la solución de los autores mejora la tasa de entrega de paquetes y el rendimiento de la red, acercándose bastante al funcionamiento de AODV sin presencia de ataques en el caso de la tasa de entrega de paquetes.

En la referencia [79], Vaseer *et al.* aseguran haber implementado el primer sistema de prevención distribuido basado en confianza para prevenir ataques múltiples. En su propuesta, unos nodos observadores determinan la confianza del resto con un mecanismo en tres pasos o estados: (i) estado de descubrimiento de ruta, (ii) estado estable y (iii) estado de ejecución. La confianza puesta en los nodos depende de las cabeceras de datos de los paquetes, siempre que sean paquetes normales de tipo Transmission Control Protocol (TCP), User Datagram Protocol (UDP) o AODV el sistema se estará comportando bien. Si las cabeceras no coinciden se marcará la situación como anormal, llegando a bloquear al nodo sospechoso. Los autores validan su propuesta en escenarios MANET simulados alcanzando unos ratios de entrega de paquetes entre 95 % y un 99 % y una tasa de falsos positivos False Positive Rate (FPR) de 35 % a 23 %.

4.3.5 Tolerancia

En general la finalidad de los distintos trabajos relacionados con las redes *Ad hoc*, en lo que respecta a su seguridad, tratan de paliar algún tipo de ataque, pero estas respuestas unas veces son más tolerantes que otras. Ya se hecho referencia a que una solución tolerante está presente durante todos los estadíos del ataque (Figura 4.16), modificando su comportamiento de acuerdo a los cambios que se producen en el sistema. Ya sean actuaciones maliciosas o no, una solución

tolerante mitigará los efectos negativos detectados acorde a los objetivos y servicios para los que se diseñó el sistema o en este caso la red. En esta subsección vamos a clasificar algunos de los trabajos que, a nuestro juicio, actúan de forma tolerante en aras de la supervivencia [41] de la red.

Por ejemplo, Su *et al.* persiguieron la idea de buscar respuestas menos estrictas. En los trabajos [73] y [71] los detectores trabajan para encontrar diferencias entres búsquedas y respuestas de ruta, con niveles de sospecha sobre los nodos. Sin embargo, cuando esos niveles de sospecha crecen la solución final es bloquear dicho nodo. De un modo similar, el método de Noguchi *et al.* [50], se basa en un umbral dinámico, tratando de ser flexible en la respuesta. Sin embargo, al traspasar el umbral, el nodo es marcado en una lista negra, evitando su participación en la MANET. Si bien es cierto que el nodo es marcado de manera temporal, con lo que podemos entender que los autores están buscando una respuesta que no sea tan drástica.

Por otro lado, tenemos respuestas como la que encontramos en [20], donde los autores buscan mitigar el ataque *Blackhole*, pero teniendo en cuenta los posibles efectos negativos utilizan múltiples rutas. Este tipo de respuesta no expulsa al nodo de la red, simplemente ignora el ataque porque lo sobrelleva. Evidentemente este mecanismo puede afectar a la eficiencia energética de la red, ya que en cierta forma se estaría realizando una inundación parcial. O trabajos como el de Nadeem *et al.* [49], cuya respuesta se basa en un sistema de castigos, en el cual los autores tuvieron en cuenta el efecto negativo del aislamiento/bloqueo del nodo malicioso en según que circunstancias. Khan *et al.* [33] formulan su trabajo para tratar de contrarrestar el agujero de gusano estableciendo no solo un umbral máximo, sino también un mínimo. En su respuesta final a un *Wormhole*, el algoritmo bloquea las comunicaciones con dicho nodo. Sin embargo, esta técnica puede resultar permisiva para un posible *Packet Dropping* que se mantenga dentro de los valores establecidos.

En [23], Geetanjali *et al.* argumentan el uso de PSO para combatir los ataques *Blackhole* y *Grayhole*. Los autores utilizan PSO para optimizar la posición de los nodos de la red de acuerdo con un valor máximo para la ruta más corta. La solución incrementa considerablemente el rendimiento de la red en términos del número total de paquetes perdidos.

Saurabh *et al.* nos proponen su solución basada en *clusters* en [63]. Se trata de una modificación del protocolo AODV, a la que simplemente han llamado Secure Ad hoc On-Demand Distance Vector (SAODV). Los nodos se agruparán en *clusters* o racimos, con un líder de grupo. Cada CH mantiene el recuento de paquetes enviados que será comprobado en destino a través de un acuse de recibo. El origen continuará enviando paquetes si, y solo si, recibe confirmación positiva desde el destino. Los autores evalúan la solución en términos de entrega de paquetes, rendimiento y retardo que mejora al clásico AODV, así como en el impacto energético, donde muestran incluso resultados mejores en SAODV.

Un trabajo que ha llamado la atención, aunque no se trate de una solución de seguridad ante amenazas o ataques, es el trabajo de Gupta *et al.* [26]. En dicho trabajo se estudia y da solución al problema del emplazamiento de nodos Relay en una red de sensores WSN, para lo que utilizan un algoritmo genético (Genetic Algorithm (GA)). En este trabajo no se intenta contrarestar ningún tipo de ataque, sin embargo, es interesante que traten de maximizar la conectividad minimizando el número de nodos Relay.

5. Conclusiones y trabajo futuro

En este capítulo se resumen las conclusiones extraídas durante el presente trabajo, y se realiza un ejercicio de reflexión acerca de hacia donde debería dirigirse la investigación en el desarrollo de nuevas soluciones de seguridad para redes *Ad hoc*, persiguiendo un enfoque tolerante.

5.1 Conclusiones

En este trabajo se ha realizado un meticuloso análisis del estado del arte en la investigación sobre seguridad en redes *Ad hoc*. Se ha realizado un análisis bibliométrico de la investigación, con el que se han extraído temáticas, tendencias y evolución de la disciplina estudiada. A través de dicho estudio se ha detectado que, entre otras temáticas, MANET y VANET son centro de atención para la comunidad investigadora, y como consecuencia, se ha centrado la búsqueda de soluciones de seguridad en el ámbito de dichas redes. Seguidamente se ha hecho una revisión sistemática de la Literatura, siguiendo la metodología de Kitchenham *et al.* [36], para ser lo más objetivos posible. Se concluye también que aunque existen trabajos que clasifican soluciones en función de unos parámetros u otros (tipos de ataques, requisitos de red, etc.) las que lo hacen por línea de defensa son pocas y no lo hacen bien. Además, se ha observado que, en líneas generales, existe un gran solape entre las medidas de prevención y detección.

Las soluciones preventivas son principalmente, desde nuestro punto de vista, aquellas basadas en técnicas criptográficas. A priori, dichas técnicas no necesitarán sistemas de detección, ya el ataque no se llega a producir. Por otro lado, tampoco sería suficiente tomar únicamente medidas de detección, ya que, si la intención final es mantener los servicios que pone la red a nuestra disposición, de poco servirá detectar un ataque si no se despliega ninguna contramedida. Tal y como Magán-Carrión *et al.* [42] concluyeron, se necesitan soluciones que actúen en todas las líneas de defensa, y que además sean capaces de tolerar el ataque. Sin embargo, tras realizar este estudio cabe mencionar la existencia de trabajos que resultan difíciles de clasificar en

una línea de defensa pura, puesto que realizan acciones en varias líneas (prevención/detección, detección/respuesta). De esta forma, lo que hemos encontrado a lo largo de esta revisión es una difusa clasificación, en términos generales, de las distintas soluciones por líneas de defensa tradicionales.

A partir de las conclusiones y trabajo anterior, se hace necesaria la propuesta de una nueva taxonomía que añade una nueva línea de defensa a las tradicionales: la tolerancia. En esta capa se engloban algunas soluciones que se basan en actuar de manera adaptativa a una amenaza o imprevisto en la red. Con esta taxonomía se pretende primero clasificar adecuadamente las soluciones existentes, y segundo abundar en el uso de soluciones tolerantes: soluciones que convivan con el ataque, pero que mitiguen sus efectos de cara a preservar los servicios para los que se diseñó el sistema. Conceptualmente hablando, las soluciones tolerantes acabarían con la necesidad de recursos basados en líneas de defensa tradicionales. Lógicamente, esto dependerá del contexto de aplicación del sistema. El uso o no de defensas menos flexibles puede venir impuesto por los propios objetivos y servicios para los que se diseñó dicho sistema. Los ataques seguirán produciéndose, solo hay que evitar que degraden el rendimiento del sistema en el sentido que sea.

Se ha observado en el análisis del estado del arte que el uso de algoritmos genéticos es muy apropiado en la búsqueda de soluciones de seguridad para redes *Ad hoc*. Por ejemplo con la idea de encontrar una solución aproximada para ubicar nodos retransmisores móviles, que suplan las deficiencias en el *Throughput* provocada por nodos maliciosos o comprometidos.

5.2 Trabajo Futuro

Al revisar el estado de la investigación, se espera tener una panorámica y obtener respuestas sobre qué debería hacerse, qué necesita mejorar y dónde están los puntos débiles de la disciplina estudiada.

Ya sabemos del intrínseco dinamismo de las redes *Ad hoc*. Un ataque puede estar afectando a un nodo durante un tiempo y luego desaparecer, o afectar a otro. Si en lugar de bloquear al nodo malicioso, se desplegara algún tipo de medida que evitara que la ruta utilizara ese nodo, se estaría hablando de una respuesta tolerante. Siendo de esta forma, no sería necesario detectar un ataque como tal, bastaría con detectar un descenso en el *throughput* de una zona concreta de la red. La línea de investigación a perseguir en futuros trabajos de seguridad para redes *Ad hoc*, en nuestra opinión, debería pasar por la búsqueda de tolerancia a la hora de dar respuesta a un comportamiento no deseado.

Como se ha visto a lo largo de la revisión, las soluciones de optimización abundan. Se desarrollan, por ejemplo, actualizaciones de protocolos de enrutamiento con la intención de optimizar dicho encaminamiento. En este sentido destacan las soluciones bioinspiradas, como es el caso del algoritmo PSO, usado frecuentemente en el contexto de las redes *Ad hoc*. La programación genética puede ser la clave para la mejora del comportamiento de los protocolos de enrutamiento para redes sin infraestructura. Por esa razón, como trabajo futuro se pretende realizar un estudio de heurísticas y algoritmos de optimización bioinspirados, así como su aplicación en soluciones de seguridad para la supervivencia de las redes *Ad hoc*. Como ya se ha

comentado, el funcionamiento de los algoritmos genéticos para encontrar soluciones aproximadas en un menor tiempo, es idóneo en un entorno altamente dinámico y cambiante como pueden ser una red MANET o VANET.

Un problema de optimización de posicionamiento de nodos Relay, por ejemplo, requiere hallar un conjunto de parámetros que hagan cumplir un cierto criterio de calidad, que es lo que se quiere optimizar (función de optimización). Ya sea minimizando (el número de nodos, el gasto energético, etc.) o maximizando (la conectividad, el rendimiento, etc.) una función de coste $f(x)$ adaptada al problema. El problema de optimización del posicionamiento de nodos Relay en un entorno de nodos en movimiento, depende del momento en el que se encuentre dicho entorno, en cada momento t se tendrá que calcular la mejor solución posible para esos nodos. Por lo que será necesaria una búsqueda de funciones de coste adecuadas a las heurísticas estudiadas que casen con las características propias de las redes *Ad hoc*, con la idea de mitigar los efectos no deseados[1]. Se tendrán en cuenta aspectos como la conectividad, PDR, End-to-end (E2E) *Delay*, *Throughput*, etc., como parámetros fundamentales.

Un siguiente paso será buscar y filtrar soluciones de seguridad en el contexto de las redes *Ad hoc* que se basen en el posicionamiento de nodos Relay. A través de entornos simulados y/o reales (si fuera posible) se pondrán a prueba esas soluciones, lo cual permitirá conocer y evaluar dichas propuestas. Se tratará de entender el comportamiento de los algoritmos desarrollados ante la presencia de diferentes tipologías de ataques. Se espera descubrir así sus fortalezas y debilidades, con la intención de encontrar formas de mejorarlo usando las citadas heurísticas bioinspiradas.

Con el aprendizaje de las mejoras de soluciones existentes, se tratará de proponer nuevas soluciones de seguridad con un enfoque superviviente, bien basadas en heurísticas y técnicas de optimización bioinspiradas y como hemos mencionado anteriormente, técnicas derivadas del aprendizaje automático o *Machine Learning* o mezcla de ambas.

[1] Se debe tener en cuenta que, para resolver un algoritmo como PSO antes de cambio de posición/tiempo se necesitará una capacidad computacional que lo permita. Lo que podría limitar la aplicación del trabajo futuro.

Bibliografía

[1] Saif Al-Sultan y col. «A comprehensive survey on vehicular Ad Hoc network». En: *Journal of Network and Computer Applications* 37.1 (2014), páginas 380-392. ISSN: 10958592. DOI: 10.1016/j.jnca.2013.02.036 (véanse páginas 76, 79, 89).

[2] Afroze Ansari y Mohammed Abdul Waheed. «Flooding attack detection and prevention in MANET based on cross layer link quality assessment». En: *Proceedings of the 2017 International Conference on Intelligent Computing and Control Systems, ICICCS 2017*. Volumen 2018-Janua. Institute of Electrical y Electronics Engineers Inc., 2017, páginas 612-617. ISBN: 9781538627457. DOI: 10.1109/ICCONS.2017.8250535 (véanse páginas 89, 97).

[3] Abderrahmane Baadache y Ali Belmehdi. «Fighting against packet dropping misbehavior in multi-hop wireless ad hoc networks». En: *Journal of Network and Computer Applications* 35.3 (2012), páginas 1130-1139. ISSN: 10848045. DOI: 10.1016/j.jnca.2011.12.012 (véanse páginas 89, 94).

[4] M. Balakrishnan y col. «Measures and countermeasures for null frequency jamming of on-demand routing protocols in wireless ad hoc networks». En: *IEEE Transactions on Wireless Communications* 11.11 (2012), páginas 3860-3868. ISSN: 15361276. DOI: 10.1109/TWC.2012.092112.110678 (véanse páginas 89, 93).

[5] *Bibliometría | OBIC (https://obic.usal.es/bibliometria)* (véase página 33).

[6] Jeremy J. Blum, Andrew Neiswender y Azim Eskandarian. «Denial of service attacks on inter-vehicle communication networks». En: *IEEE Conference on Intelligent Transportation Systems, Proceedings, ITSC*. 2008, páginas 797-802. DOI: 10.1109/ITSC.2008.4732612 (véanse páginas 30, 89).

[7] M. Callon, J. P. Courtial y F. Laville. «Co-word analysis as a tool for describing the network of interactions between basic and technological research: The case of polymer chemsitry». En: *Scientometrics* 22.1 (1991), páginas 155-205. ISSN: 01389130. DOI:

10.1007/BF02019280. URL: http://link.springer.com/10.1007/BF02019280 (véase página 41).

[8] Michel Callon y col. «From translations to problematic networks: An introduction to co-word analysis». En: *Social Science Information* (1983). ISSN: 14617412. DOI: 10.1177/053901883022002003 (véase página 39).

[9] Rohit Chourasia y Rajesh Kumar Boghey. «Novel IDS security against attacker routing misbehavior of packet dropping in MANET». En: *Proceedings of the 7th International Conference Confluence 2017 on Cloud Computing, Data Science and Engineering*. Institute of Electrical y Electronics Engineers Inc., 2017, páginas 456-460. ISBN: 9781509035182. DOI: 10.1109/CONFLUENCE.2017.7943194 (véanse páginas 30, 89, 95).

[10] Paul Loh Ruen Chze, Wayne Kan Wai Yan y Kan Siew Leong. «A user-controllable multi-layer secure algorithm for MANET». En: *IWCMC 2012 - 8th International Wireless Communications and Mobile Computing Conference*. 2012, páginas 1080-1084. ISBN: 9781457713781. DOI: 10.1109/IWCMC.2012.6314356 (véanse páginas 89, 93).

[11] M.J. Cobo y col. «An approach for detecting, quantifying, and visualizing the evolution of a research field: A practical application to the Fuzzy Sets Theory field». En: *Journal of Informetrics* 5 (2011), páginas 146-166. ISSN: 17511577. DOI: 10.1016/j.joi.2010.10.002. URL: https://linkinghub.elsevier.com/retrieve/pii/S1751157710000891 (véanse páginas 40, 43).

[12] M.J. Cobo y col. «Science mapping software tools: Review, analysis, and cooperative study among tools». En: *Journal of the American Society for Information Science and Technology* 62.7 (2011), páginas 1382-1402. ISSN: 15322882. DOI: 10.1002/asi.21525. URL: http://doi.wiley.com/10.1002/asi.21525 (véase página 37).

[13] M.J. Cobo y col. «SciMAT: A new science mapping analysis software tool». En: *Journal of the American Society for Information Science and Technology* 63.8 (2012), páginas 1609-1630. ISSN: 15322882. DOI: 10.1002/asi.22688. URL: http://doi.wiley.com/10.1002/asi.22688 (véanse páginas 30, 39).

[14] Manuel Jesús Cobo Martín. «SciMat: herramienta software para el análisis de la evolución del conocimiento científico. Propuesta de una metodología de evaluación». Tesis doctoral. 2011. ISBN: 9788469510698. URL: http://hdl.handle.net/10481/20201 (véase página 37).

[15] Neal Coulter. «Software engineering as seen through its research literature: A study in co-word analysis». En: *Journal of the American Society for Information Science* (1998). ISSN: 00028231. DOI: 10.1002/(sici)1097-4571(1998)49:13<1206::aid-asi7>3.3.co;2-6 (véase página 41).

[16] Semih Dokurer, Y. M. Erten y Can Erkin Acar. «Performance analysis of ad-hoc networks under black hole attacks». En: *Conference Proceedings - IEEE SOUTHEASTCON*. 2007, páginas 148-153. ISBN: 1424410290. DOI: 10.1109/SECON.2007.342872 (véanse páginas 28, 89, 92).

[17] Ali Dorri. «An EDRI-based approach for detecting and eliminating cooperative black hole nodes in MANET». En: *Wireless Networks* 23.6 (2017), páginas 1767-1778. ISSN: 15728196. DOI: 10.1007/s11276-016-1251-x (véanse páginas 89, 94).

[18] Russell Eberhart y James Kennedy. «New optimizer using particle swarm theory». En: *Proceedings of the International Symposium on Micro Machine and Human Science*. IEEE, 1995, páginas 39-43. DOI: 10.1109/mhs.1995.494215. URL: https://ieeexplore.ieee.org/document/494215 (véase página 30).

[19] Nees Jan van Eck y Ludo Waltman. «How to normalize cooccurrence data? An analysis of some well-known similarity measures». En: *Journal of the American Society for Information Science and Technology* 60.8 (2009), páginas 1635-1651. ISSN: 15322882. DOI: 10.1002/asi.21075. URL: http://doi.wiley.com/10.1002/asi.21075 (véase página 40).

[20] Elbasher Elmahdi, Seong-Moo Yoo y Kumar Sharshembiev. «Secure and reliable data forwarding using homomorphic encryption against blackhole attacks in mobile ad hoc networks». En: *Journal of Information Security and Applications* 51 (2020), página 102425. ISSN: 22142126. DOI: 10.1016/j.jisa.2019.102425. URL: https://linkinghub.elsevier.com/retrieve/pii/S2214212618303879 (véanse páginas 89, 98).

[21] Richard Gilles Engoulou y col. «VANET security surveys». En: *Computer Communications* 44 (2014), páginas 1-13. ISSN: 01403664. DOI: 10.1016/j.comcom.2014.02.020 (véanse páginas 77, 79, 89).

[22] Pedro García Teodoro y Gabriel Maciá Fernández. *Seguridad en redes y sistemas de comunicación: teoría y práctica*. Spanish. Independently Published, 2020. ISBN: 9798605091257 (véase página 89).

[23] Geetanjali y Jyoti Gupta. «Improved approach of co-operative gray hole attack prevention monitored by meta heuristic on MANET». En: *4th IEEE International Conference on Signal Processing, Computing and Control, ISPCC 2017*. Volumen 2017-Janua. Institute of Electrical y Electronics Engineers Inc., 2017, páginas 356-361. ISBN: 9781509058389. DOI: 10.1109/ISPCC.2017.8269703 (véanse páginas 89, 98).

[24] Amrita Ghosal y Mauro Conti. «Security issues and challenges in V2X: A Survey». En: *Computer Networks* 169 (2020), páginas 1-20. ISSN: 1389-1286. DOI: 10.1016/j.comnet.2019.1070931389-1286 (véanse páginas 77, 80, 89).

[25] Qijun Gu. «Packet-Dropping Attack». En: *Encyclopedia of Cryptography and Security*. Editado por Henk C. A. van Tilborg y Sushil Jajodia. Boston, MA: Springer US, 2011, páginas 899-902. ISBN: 978-1-4419-5906-5. DOI: 10.1007/978-1-4419-5906-5_635. URL: https://doi.org/10.1007/978-1-4419-5906-5_635 (véase página 30).

[26] Suneet K. Gupta, Pratyay Kuila y Prasanta K. Jana. «Genetic algorithm for k-connected relay node placement in wireless sensor networks». En: *Advances in Intelligent Systems and Computing*. Volumen 379. Springer Verlag, 2016, páginas 721-729. ISBN: 9788132225164. DOI: 10.1007/978-81-322-2517-1_69 (véase página 99).

[27] Badis Hammi y col. «A secure multipath reactive protocol for routing in IoT and HANETs». En: *Ad Hoc Networks* 103 (2020). ISSN: 15708705. DOI: 10.1016/j.adhoc.2020.102118 (véase página 28).

[28] Frederic L. Holmes. «Scientific Writing and Scientific Discovery». En: *Isis* 78.2 (1987), páginas 220-235. ISSN: 0021-1753. DOI: 10.1086/354391. URL: https://www.journals.uchicago.edu/doi/10.1086/354391 (véase página 20).

[29] IEEE Standard for Information technology. *802.11s-2011 - IEEE Standard for Information Technology–Telecommunications and information exchange between systems–Local and metropolitan area networks–Specific requirements Part 11: Amendment 10: Mesh Networking*. 2011. DOI: 10.1109/IEEESTD.2011.6018236. URL: http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp={\&}arnumber=6018236{\&}contentType=Standards{\&}sortType=asc{_}p{_}Sequence{\&}filter=AND(p{_}Publication{_}Number:6018234) (véase página 27).

[30] Lincy Elizebeth Jim y Mark A. Gregory. «A Review of Artificial Immune System Based Security Frameworks for MANET». En: *International Journal of Communications, Network and System Sciences* 09.01 (2016), páginas 1-18. ISSN: 1913-3715. DOI: 10.4236/ijcns.2016.91001 (véanse páginas 77, 79, 89).

[31] Avita Katal y col. «A cluster based detection and prevention mechanism against novel datagram chunk dropping attack in MANET multimedia transmission». En: *2013 IEEE Conference on Information and Communication Technologies, ICT 2013*. 2013, páginas 479-484. ISBN: 9781467357586. DOI: 10.1109/CICT.2013.6558143 (véanse páginas 30, 89, 95).

[32] Chaker Abdelaziz Kerrache y col. «Trust Management for Vehicular Networks: An Adversary-Oriented Overview». En: 4 (2016), páginas 9293-9307. ISSN: 21693536. DOI: 10.1109/ACCESS.2016.2645452 (véanse páginas 76, 79, 89).

[33] Farrukh Aslam Khan y col. «A detection and prevention system against collaborative attacks in Mobile Ad hoc Networks». En: *Future Generation Computer Systems* 68 (2017), páginas 416-427. ISSN: 0167739X. DOI: 10.1016/j.future.2016.07.010 (véanse páginas 89, 96, 98).

[34] Nitin Khanna y Monika Sachdeva. «A comprehensive taxonomy of schemes to detect and mitigate blackhole attack and its variants in MANETs». En: *Computer Science Review* 32 (2019), páginas 24-44. ISSN: 15740137. DOI: 10.1016/j.cosrev.2019.03.001 (véanse páginas 77, 80, 89).

[35] Barbara Kitchenham. «Procedures for performing systematic reviews». En: *Keele University,UK and National ICT Australia* (2004). ISSN: 13537776. DOI: 10.1.1.122.3308 (véanse páginas 45, 57).

[36] S Kitchenham, B. and Charters. «Guidelines for performing systematic literature reviews in software engineering». En: *Technical report, Ver. 2.3 EBSE Technical Report. EBSE* () (véanse páginas 30, 35, 44-46, 57, 101).

[37] Sachin Korde y M. V. Sarode. «Review on network layer attacks detection and prevention techniques in mobile ad hoc networks». En: *Proceedings of the International Conference on Inventive Systems and Control, ICISC 2017*. Institute of Electrical y Electronics Engineers Inc., 2017. ISBN: 9781509047154. DOI: 10.1109/ICISC.2017.8068654 (véanse páginas 30, 78, 80, 89).

[38] Edward A. Lee. *Cyber Physical Systems: Design Challenges*. Informe técnico UCB/EECS-2008-8. EECS Department, University of California, Berkeley, 2008. URL: http://www2.eecs.berkeley.edu/Pubs/TechRpts/2008/EECS-2008-8.html (véase página 70).

[39] Wenjia Li y Houbing Song. «ART: An Attack-Resistant Trust Management Scheme for Securing Vehicular Ad Hoc Networks». En: *IEEE Transactions on Intelligent Transportation Systems* 17.4 (abr. de 2016), páginas 960-969. ISSN: 1558-0016. DOI: 10.1109/TITS.2015.2494017 (véanse páginas 89, 94).

[40] X. Li y col. «Trust-based on-demand multipath routing in mobile ad hoc networks». En: *IET Information Security* 4.4 (2010), páginas 212-232. ISSN: 17518709. DOI: 10.1049/iet-ifs.2009.0140 (véanse páginas 30, 89, 93, 96).

[41] M. Lima, Aldri Luiz Dos Santos y Guy Pujolle. «A survey of survivability in mobile Ad hoc Networks». En: *IEEE Communications Surveys and Tutorials* 11.1 (2009), páginas 66-77. ISSN: 1553877X. DOI: 10.1109/SURV.2009.090106. URL: http://ieeexplore.ieee.org/document/4796927 (véanse páginas 90, 98).

[42] Roberto Magan-Carrion. «Seguridad para la supervivencia en redes ad hoc». En: *Supervivencia en redes ad hoc. Mecanismos de tolerancia y reacción frente amenazas de seguridad.* Universidad de Granada, 2016. ISBN: 9788491259138. URL: http://hdl.handle.net/10481/43857 (véanse páginas 30, 78, 80, 89, 90, 101).

[43] Roberto Magán-Carrión y col. «Towards a reliable comparison and evaluation of network intrusion detection systems based on machine learning approaches». En: *Applied Sciences (Switzerland)* 10.5 (2020), página 1775. ISSN: 20763417. DOI: 10.3390/app10051775. URL: https://www.mdpi.com/2076-3417/10/5/1775 (véase página 90).

[44] Mohamed Nidhal Mejri, Jalel Ben-Othman y Mohamed Hamdi. «Survey on VANET security challenges and possible cryptographic solutions». En: *Vehicular Communications* 1.2 (2014), páginas 53-66. ISSN: 22142096. DOI: 10.1016/j.vehcom.2014.05.001 (véanse páginas 76, 79, 89).

[45] C. Aguilar Melchor y col. «Ant trust: A novel ant routing protocol for wireless ad-hoc network based on trust between nodes». En: *ARES 2008 - 3rd International Conference on Availability, Security, and Reliability, Proceedings*. 2008, páginas 1052-1059. ISBN: 0769531024. DOI: 10.1109/ARES.2008.110 (véanse páginas 30, 89, 92).

[46] Monika Mistry, Purvi Tandel y Vijay Reshamwala. «Mitigating techniques of black hole attack in MANET: A review». En: *Proceedings - International Conference on Trends in Electronics and Informatics, ICEI 2017*. Volumen 2018-Janua. Institute of Electrical y Electronics Engineers Inc., 2018, páginas 554-557. ISBN: 9781509042579. DOI: 10.1109/ICOEI.2017.8300721 (véanse páginas 78, 80, 89).

[47] S. Muthurajkumar y col. «An Intelligent Secured and Energy Efficient Routing Algorithm for MANETs». En: *Wireless Personal Communications* 96.2 (2017), páginas 1753-1769. ISSN: 1572834X. DOI: 10.1007/s11277-017-4266-4 (véanse páginas 30, 89, 96).

[48] Ahmed Nabet y col. «Towards secure route discovery protocol in MANET». En: *Global Information Infrastructure Symposium, GIIS 2011*. 2011, páginas 1-8. ISBN: 9781457712623. DOI: 10.1109/GIIS.2011.6026717 (véanse páginas 30, 89, 93).

[49] Adnan Nadeem y Michael P. Howarth. «An intrusion detection & adaptive response mechanism for MANETs». En: *Ad Hoc Networks* 13.PART B (2014), páginas 368-380. ISSN: 15708705. DOI: 10.1016/j.adhoc.2013.08.017 (véanse páginas 30, 89, 96, 98).

[50] Taku Noguchi y Takaya Yamamoto. «Black hole attack prevention method using dynamic threshold in mobile ad hoc networks». En: *Proceedings of the 2017 Federated Conference on Computer Science and Information Systems, FedCSIS 2017*. Institute of Electrical y Electronics Engineers Inc., 2017, páginas 797-802. ISBN: 9788394625375. DOI: 10.15439/2017F101 (véanse páginas 89, 97, 98).

[51] E.C.M. Noyons, H.F. Moed y M. Luwel. «Combining mapping and citation analysis for evaluative bibliometric purposes: A bibliometric study». En: *Journal of the American Society for Information Science* 50.2 (1999), páginas 115-131. ISSN: 0002-8231. DOI: 10.1002/(SICI)1097-4571(1999)50:2<115::AID-ASI3>3.0.CO;2-J. URL: https://onlinelibrary.wiley.com/doi/10.1002/(SICI)1097-4571(1999)50:2{\%}3C115::AID-ASI3{\%}3E3.0.CO;2-J (véase página 37).

[52] Nirav J. Patel y Rutvij H. Jhaveri. «Trust based approaches for secure routing in VANET: A survey». En: *Procedia Computer Science*. Volumen 45. C. Elsevier B.V., 2015, páginas 592-601. DOI: 10.1016/j.procs.2015.03.112 (véanse páginas 75, 79, 89).

[53] Charles E. Perkins y Elizabeth M. Royer. «Ad-hoc on-demand distance vector routing». En: *Proceedings - WMCSA'99: 2nd IEEE Workshop on Mobile Computing Systems and Applications*. 1999, páginas 90-100. ISBN: 0769500250. DOI: 10.1109/MCSA.1999.749281 (véase página 31).

[54] Ponemon Institute. «2018 cost of a data breach study: Global Overview». En: *IBM Security Services* July (2018), página 76. URL: https://www.ibm.com/downloads/cas/861MNWN2 (véase página 90).

[55] Anthony F.J. van Raan. «Measuring Science». En: *Handbook of Quantitative Science and Technology Research*. Springer Netherlands, 2004, páginas 19-50. DOI: 10.1007/1-4020-2755-9_2. URL: https://link.springer.com/chapter/10.1007/1-4020-2755-9{_}2 (véase página 37).

[56] Murad A. Rassam y col. «A sinkhole attack detection scheme in Mintroute wireless Sensor Networks». En: *2012 International Symposium on Telecommunication Technologies, ISTT 2012*. 2012, páginas 71-75. ISBN: 9781467347860. DOI: 10.1109/ISTT.2012.6481568 (véase página 92).

[57] *Real Academia Española, "Procedencia y significado del término ad hoc."* URL: http://lema.rae.es/dpd/srv/search?key=hoc (visitado 27-11-2019) (véase página 27).

[58] Aqeel-ur Rehman, Sadiq Ur Rehman y Haris Raheem. «Sinkhole Attacks in Wireless Sensor Networks: A Survey». En: *Wireless Personal Communications* 106.4 (2019), páginas 2291-2313. ISSN: 0929-6212. DOI: 10.1007/s11277-018-6040-7. URL: https://doi.org/10.1007/s11277-018-6040-7 (véase página 92).

[59] NHS Centre for Reviews y Dissemination. *Undertaking systematic reviews of research on effectiveness: CRD's guidance for those carrying out or commissioning reviews*. 2001 (véase página 47).

[60] R. L. Rivest, A. Shamir y L. Adleman. «A method for obtaining digital signatures and public-key cryptosystems». En: *Communications of the ACM* 21.2 (1978), páginas 120-126. ISSN: 00010782. DOI: 10.1145/359340.359342. URL: http://portal.acm.org/citation.cfm?doid=359340.359342 (véase página 64).

[61] Kimaya Sanzgiri y col. «Authenticated routing for ad hoc networks». En: *IEEE Journal on Selected Areas in Communications* 23.3 (2005), páginas 598-609. ISSN: 07338716. DOI: 10.1109/JSAC.2004.842547 (véanse páginas 89, 92).

[62] Anjali Sardana y col. «Black hole attack's effect mobile ad-hoc networks (MANET)». En: *Conference Proceeding - 2015 International Conference on Advances in Computer Engineering and Applications, ICACEA 2015*. Institute of Electrical y Electronics Engineers Inc., 2015, páginas 966-970. ISBN: 9781467369114. DOI: 10.1109/ICACEA.2015.7164846 (véanse páginas 76, 79, 89).

[63] Vidya Kumari Saurabh y col. «Cluster-based technique for detection and prevention of black-hole attack in MANETs». En: *Proceedings of the International Conference on Electronics, Communication and Aerospace Technology, ICECA 2017*. Volumen 2017-Janua. Institute of Electrical y Electronics Engineers Inc., 2017, páginas 489-494. DOI: 10.1109/ICECA.2017.8212712 (véanse páginas 30, 89, 98).

[64] Aumreesh Ku Saxena, Sitesh Sinha y Piyush Shukla. «A review on intrusion detection system in mobile ad-hoc network». En: *International Conference on Recent Innovations in Signal Processing and Embedded Systems, RISE 2017*. Volumen 2018-Janua. Institute of Electrical y Electronics Engineers Inc., 2018, páginas 549-554. ISBN: 9781509047604. DOI: 10.1109/RISE.2017.8378216 (véanse páginas 77, 80, 89).

[65] Jaydip Sen, Sripad Koilakonda y Arijit Ukil. «A mechanism for detection of cooperative black hole attack in mobile ad hoc networks». En: *Proceedings - 2011 2nd International Conference on Intelligent Systems, Modelling and Simulation, ISMS 2011*. 2011, páginas 338-343. ISBN: 9780769543369. DOI: 10.1109/ISMS.2011.58 (véase página 95).

[66] Henry Small. «Co-citation in the scientific literature: A new measure of the relationship between two documents». En: *Journal of the American Society for Information Science* (1973). ISSN: 10974571. DOI: 10.1002/asi.4630240406 (véase página 39).

[67] Henry Small. «Tracking and predicting growth areas in science». En: *Scientometrics*. 2006. DOI: 10.1007/s11192-006-0132-y (véase página 38).

[68] Henry Small y Phineas Upham. «Citation structure of an emerging research area on the verge of application». En: *Scientometrics* (2009). ISSN: 01389130. DOI: 10.1007/s11192-009-0424-0 (véase página 38).

[69] Henry G Small. «A Co-Citation Model of a Scientific Specialty: A Longitudinal Study of Collagen Research». En: *Social Studies of Science* 7.2 (1977), páginas 139-166. ISSN: 14603659. DOI: 10.1177/030631277700700202. URL: http://journals.sagepub.com/doi/10.1177/030631277700700202 (véase página 43).

[70] Seyed Ahmad Soleymani y col. «Trust management in vehicular ad hoc network: a systematic review». En: *Eurasip Journal on Wireless Communications and Networking* 2015.1 (2015). ISSN: 16871499. DOI: 10.1186/s13638-015-0353-y (véanse páginas 75, 79, 89).

[71] Ming Yang Su. «Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection systems». En: *Computer Communications* 34.1 (2011), páginas 107-117. ISSN: 01403664. DOI: 10.1016/j.comcom.2010.08.007 (véanse páginas 30, 89, 95, 98).

[72] Ming Yang Su y Kun Lin Chiang. «Prevention of wormhole attacks in mobile Ad Hoc networks by intrusion detection nodes». En: *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*. Volumen 6221 LNCS. Springer, Berlin, Heidelberg, 2010, páginas 253-260. ISBN: 3642146538. DOI: 10.1007/978-3-642-14654-1_31 (véanse páginas 89, 96).

[73] Ming Yang Su, Kun Lin Chiang y Wei Cheng Liao. «Mitigation of black-hole nodes in mobile ad hoc networks». En: *Proceedings - International Symposium on Parallel and Distributed Processing with Applications, ISPA 2010*. 2010, páginas 162-167. ISBN: 9780769541907. DOI: 10.1109/ISPA.2010.74 (véanse páginas 30, 89, 95, 98).

[74] Seryvuth Tan y Keecheon Kim. «Secure route discovery for preventing black hole attacks on AODV-based MANETs». En: *Proceedings - 2013 IEEE International Conference on High Performance Computing and Communications, HPCC 2013 and 2013 IEEE International Conference on Embedded and Ubiquitous Computing, EUC 2013*. IEEE Computer Society, 2014, páginas 1159-1164. ISBN: 9780769550886. DOI: 10.1109/HPCC.and.EUC.2013.164 (véanse páginas 89, 97).

[75] Shrikant S. Tangade y Sunilkumar S. Manvi. «A survey on attacks, security and trust management solutions in VANETs». En: *2013 4th International Conference on Computing, Communications and Networking Technologies, ICCCNT 2013*. 2013. ISBN: 9781479939268. DOI: 10.1109/ICCCNT.2013.6726668 (véanse páginas 75, 79, 89).

[76] S. Phineas Upham y Henry Small. «Emerging research fronts in science and technology: Patterns of new knowledge development». En: *Scientometrics* (2010). ISSN: 01389130. DOI: 10.1007/s11192-009-0051-9 (véase página 38).

[77] S. Phineas Upham y Henry Small. «Emerging research fronts in science and technology: Patterns of new knowledge development». En: *Scientometrics* (2010). ISSN: 01389130. DOI: 10.1007/s11192-009-0051-9 (véase página 38).

[78] S. Phineas Upham y Henry Small. «Emerging research fronts in science and technology: Patterns of new knowledge development». En: *Scientometrics* (2010). ISSN: 01389130. DOI: 10.1007/s11192-009-0051-9 (véase página 38).

[79] Gurveen Vaseer, Garima Ghai y Dhruva Ghai. «Distributed trust-based multiple attack prevention for secure MANETs». En: *Proceedings - 2018 IEEE 4th International Symposium on Smart Electronic Systems, iSES 2018*. Institute of Electrical y Electronics Engineers Inc., 2018, páginas 108-113. ISBN: 9781538691724. DOI: 10.1109/iSES.2018.00032 (véanse páginas 89, 97).

[80] *Vehicular networking: A survey and tutorial on requirements, architectures, challenges, standards and solutions*. 2011. DOI: 10.1109/SURV.2011.061411.00019 (véanse páginas 30, 75, 79, 89).

[81] Roshani Verma, Roopesh Sharma y Upendra Singh. «New approach through detection and prevention of wormhole attack in MANET». En: *Proceedings of the International Conference on Electronics, Communication and Aerospace Technology, ICECA 2017*. Volumen 2017-Janua. Institute of Electrical y Electronics Engineers Inc., 2017, páginas 526-531. DOI: 10.1109/ICECA.2017.8212719 (véanse páginas 89, 95).

[82] Xia Ye, Junshan Li y Rong Luo. «Hide Markov Model based intrusion detection and response for manets». En: *Proceedings - 2nd International Conference on Information Technology and Computer Science, ITCS 2010*. 2010, páginas 142-145. ISBN: 9780769540740. DOI: 10.1109/ITCS.2010.41 (véanse páginas 30, 89, 94).

[83] Dan York. «Eavesdropping and Modification». En: *Seven Deadliest Unified Communications Attacks*. Elsevier, 2010, páginas 41-69. DOI: 10.1016/b978-1-59749-547-9.00003-x. URL: https://www-sciencedirect-com/science/article/pii/B978159749547900003X (véase página 93).

[84] Sherali Zeadally y col. «Vehicular ad hoc networks (VANETS): status, results, and challenges». En: *Telecommunication Systems* 50.4 (2012), páginas 217-241. ISSN: 1018-4864. DOI: 10.1007/s11235-010-9400-5 (véanse páginas 76, 79, 89).

A. Anexo

A.1 Categorías de ataques tipificados

Los ataques se clasifican según el perjuicio que provocan en la red, así habrá ataques activos o pasivos. Se señalan a continuación algunos de los ataques más comunes en el contexto de las redes *Ad hoc* agrupados en activos y pasivos.

- **Activos**
  Tienen la intención de interferir en el funcionamiento normal de la red provocando desconexiones de alguna manera.
  - **Sinkhole**
    El efecto sumidero consiste en que un nodo comprometido de la red trata de atraer todo el tráfico hacia él anunciando falso enrutamiento. Este tipo de ataque suele ser la antesala para otras amenazas como pueden ser el *Selective Forwarding*, el *Acknowledge Spoofing* o el *Packet Dropping*. Esta última afecta de manera especial a las redes *Ad hoc* y se comenta a continuación. En la Figura A.1 se ve un ejemplo conceptual de lo que sería un *Sinkhole* atrayendo el tráfico de la red.
  - **Packet Dropping**
    El *Packet Dropping* consiste en descartar paquetes deliberadamente. Existen varias modalidades de ataques que cumplen con esta situación. En la Figura A.2 se ven algunos ejemplos de lo que sería el flujo normal (Subfigura A.2(a)), un *Blackhole* que descarta toda la información recibida (Subfigura A.2(b)), un *Grayhole* que descarta algunos paquetes y reenvía otros (Subfigura A.2(c)) y un *Grayhole* colaborativo (Subfigura A.2(d)) que reenvía los paquetes que serán descartados al autentico *Blackhole*.

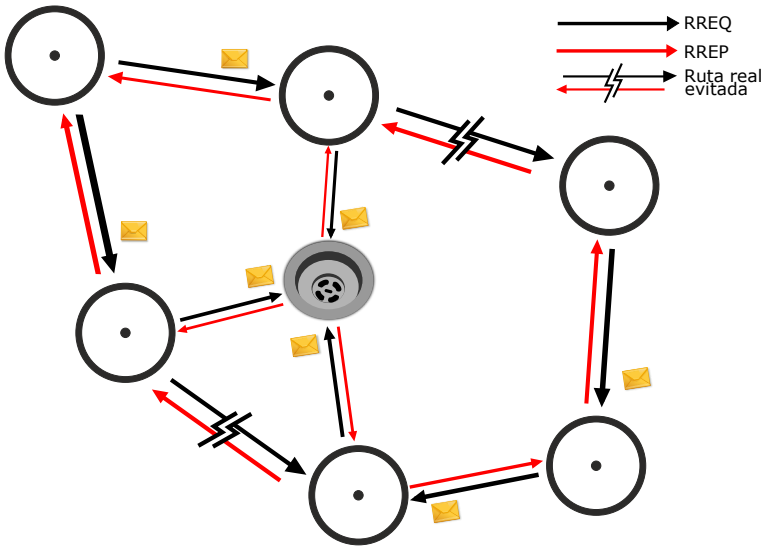


Figura A.1: Ejemplo de efecto sumidero *Sinkhole*.

- **Wormhole**
  Como decíamos, tras un *Sinkhole* se ocultan distintas intenciones. Una vez atraído el tráfico de la red hacia él, la información se descarta, se modifica o se reenvía a un tercero que tendrá sus propias intenciones. Como el *Black/Grey-hole* colaborativo, a esta acción también se la conoce como agujero de gusano o *wormhole*. En la Figura A.3 se observa un ejemplo conceptual de esta amenaza.
- **DoS (Denial of Service)**
  La denegación de servicios consiste en introducir en la red elementos que agoten deliberadamente los recursos de uno o más nodos. Normalmente se hace un envío masivo de Mensaje *HELLO* o con información inútil. En la Figura A.4 se observa un ejemplo de inundación por paquetes *SPAM* con la intención de agotar la batería de uno de los nodos legítimos.
- **Jamming: Interferencias**
  Un elemento emisor de interferencias supone un perjuicio considerable a razón del alcance de que disponga. Cualquier nodo legítimo dentro de su rango de acción puede quedar desconectado de la red. En la Figura A.5 se observa un ejemplo de un emisor de interferencias provocando la desconexión parcial de la red.
- **Modification: Modificación**
  Este ataque consiste en modificar intencionadamente la información que pasa por un nodo comprometido antes de reenviarla. Lo normal es que dicho nodo esté actuando como *Man-in-The-Middle*, explicado en la siguiente sección como ataque pasivo. En la Figura A.6 se muestra un ejemplo de un nodo recibiendo paquetes y modificándolos antes de reenviarlos.

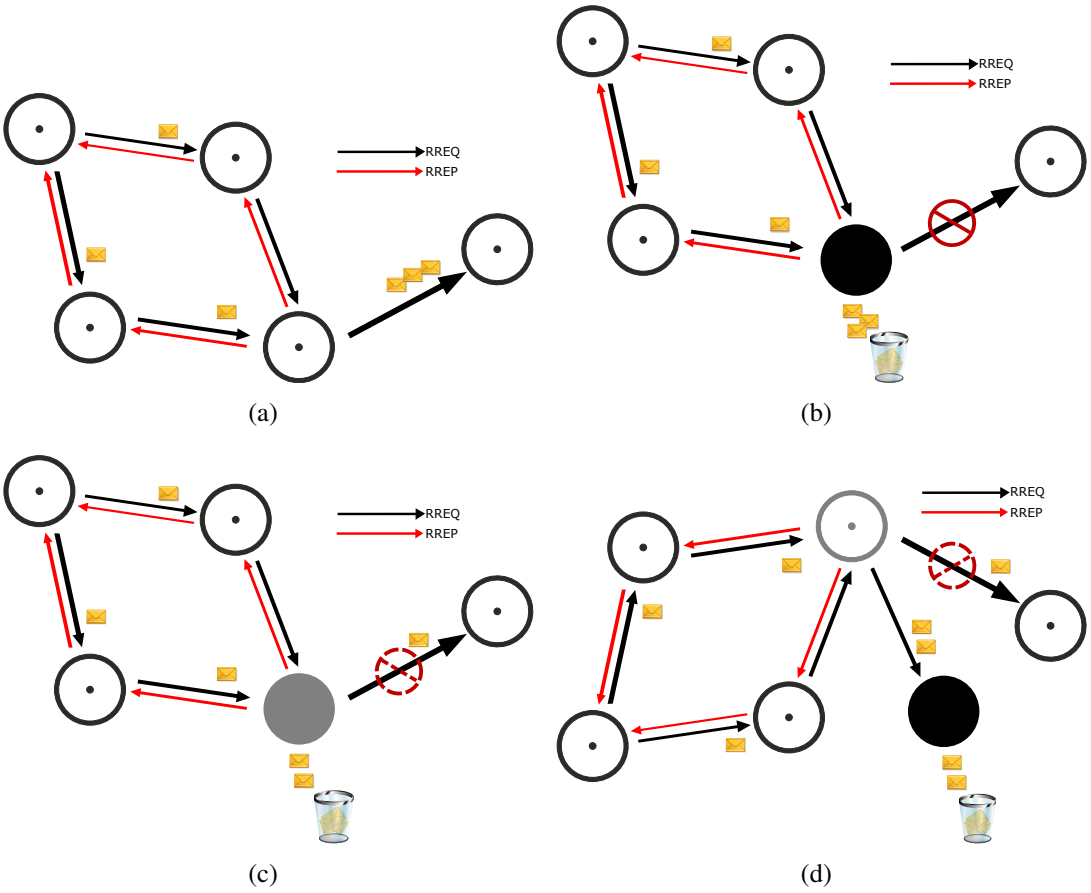


Figura A.2: Ejemplos de Packet Dropping. Figura A.2(a) flujo normal. Figura A.2(b) agujero negro. Figura A.2(c) agujero gris. Figura A.2(d) agujero gris/negro colaborativo.

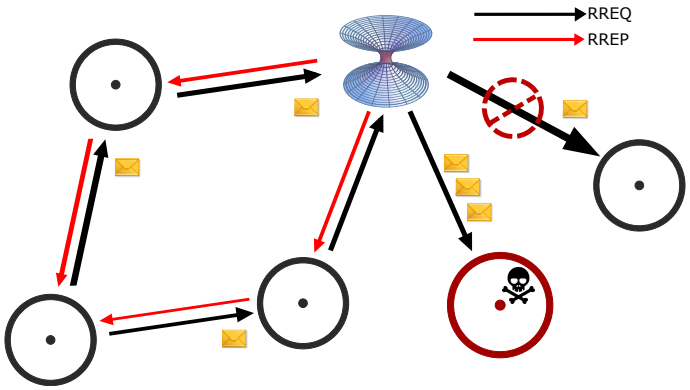


Figura A.3: Ejemplo de *Wormhole*.

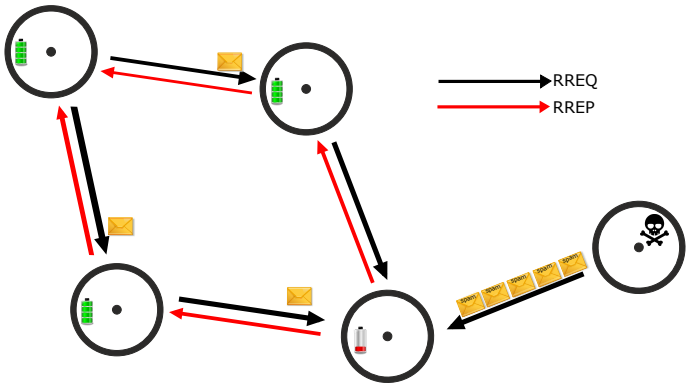


Figura A.4: Ejemplo de inundación por paquetes *SPAM*.

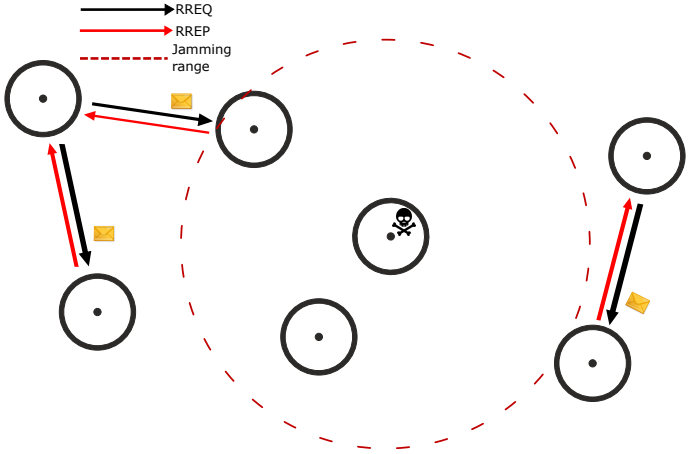


Figura A.5: Ejemplo de desconexión por interferencias.

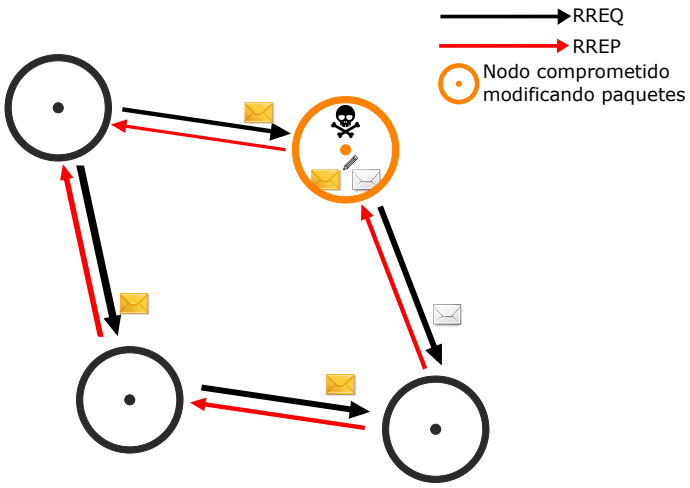
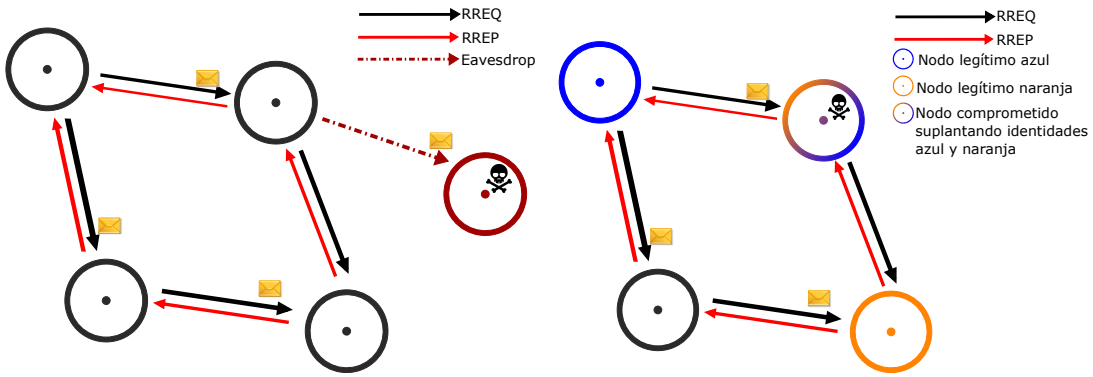


Figura A.6: Ejemplo de modificación de paquetes.

- **Pasivos**
  Tratan de escuchar las comunicaciones sin ser descubiertos.
  - **Eavesdropping: escuchando a escondidas**
    El término *eavesdrop*[1] quiere decir literalmente escuchar a escondidas. Y eso es exactamente lo que hace el nodo, capturar la información a su alcance sin permiso y en secreto. En la Figura A.7(a) se observa un ejemplo de escucha no autorizada.



(a) (b)

Figura A.7: Ejemplos de ataques pasivos, en la Figura A.7(a) se ve un ejemplo de escucha no autorizada, mientras en la Figura A.7(b) se ve un ejemplo de *Man in the middle*.

  - **MiTM (Man in The Middle)**
    Ataque en el cual el nodo malicioso trata de colocarse entre emisor y receptor de una conexión suplantando la identidad de uno de ellos o de ambos. El Man-in-The-Middle (MiTM) Puede ser la antesala de un ataque de modificación. En la Figura A.7(b) se observa un ejemplo en el que un nodo malicioso esta suplantando la identidad de otros dos.

[1] Según El Oxford English Dictionary. Eavesdrop verb: to listen secretly to what other people are saying.

.

Resumen/Abstract

En el mundo conectado en el que vivimos hoy en día, las redes ad hoc juegan un papel muy importante. Sin embargo, son sus principales características las que las hacen vulnerables desde el punto de vista de la seguridad. Es por esto por lo que el presente trabajo se centra en el estudio de la seguridad en este tipo de redes. Así, se ha realizado un análisis bibliométrico para detectar las temáticas mas relevantes y la evolución de la investigación en lo que concierne a la seguridad en redes ad hoc, que muestra, primero, que el campo de estudio sigue activo, y segundo, que las temáticas MANET y VANET son centro de atención. A partir de aquí, se ha realizado una revisión sistemática de la Literatura centrada en la seguridad en redes MANET y VANET y cómo los trabajos del estado del arte clasifican las soluciones encontradas acorde a las principales líneas de defensa: prevención, detección y respuesta. Si bien, abundan las soluciones de detección de ataques o intrusiones, existe cierta confusión a la hora de enmarcar dichas soluciones por línea de defensa. Así, se ha propuesto una nueva taxonomía que, desde nuestro punto de vista, mejora la clasificación tradicional por línea de defensa añadiendo nuevas como la tolerancia. Finalmente, concluimos con la necesidad de la propuesta de soluciones tolerantes que, bien planteadas, mitiguen los efectos del ataque sin necesidad de una detección y una respuesta real, minimizando así el impacto producido por un atacante en el sistema.

Nowadays, we are living in a connected world, where ad hoc networks perform an important role. However, their main characteristics are in turn their main security weaknesses. Because of that, the current work surveys the security in ad hoc networks. This way, a bibliometric analysis has been carried out to detect the most relevant topics and the evolution of research in terms of security in ad hoc networks, from which it has been shown, first, the field of study remains active, and second, the themes MANET and VANET are a study centre. With this information, a systematic Literature review has been carried out mainly focused on the security in MANETs and VANETs and how the current state of the art solutions are classified by traditional defence lines: prevention, detection or response. From this preliminary study we realized that it is hard to split solutions into one the previous defence lines. As a consequence, we introduced here a novel taxonomy that goes beyond the traditional one and introduce new defence lines, e.g., the tolerance. Finally, from our point of view, much more work should be done in the proposal of tolerance approaches by the research community. This kind of solutions could even make the use of detection and response-based solutions unnecessary, thus minimizing the impact of attacks on the system.

UNIVERSIDAD DE ALMERÍA

MÁSTER EN TECNOLOGÍAS Y APLICACIONES EN INGENIERÍA INFORMÁTICA