Líneas de Defensa y Seguridad en Redes ad hoc: un Estudio Sistemático

Juan Antonio Rodríguez Baeza
Dpto. de Ingeniería Informática
Universidad de Cádiz
{juanantonio.rodriguez@uca.es}

Roberto Magán Carrión
Dpto. de Teoría de la Señal
Telemática y Comunicaciones
Universidad de Granada
{rmagan@ugr.es}

Patricia Ruíz Villalobos
Dpto. de Ingeniería Mecánica
y Diseño Industrial
Universidad de Cádiz
{patricia.ruiz@uca.es}

***Resumen*—**
Hoy día vivimos en un mundo hiperconectado, donde coexisten diversidad de aplicaciones y servicios que se soportan en gran medida a través de la utilización de redes ad hoc. Estas redes descentralizadas son tan flexibles y versátiles como vulnerables, siendo objeto de multitud de amenazas y ataques de seguridad. Este trabajo presenta un meticuloso estudio sobre el estado del arte actual y tendencias en el contexto de la seguridad en este tipo de redes. Para ello se han utilizado metodologías derivadas del análisis bibliométrico como el *Science Mapping*, así como aquellas que guían el proceso de revisión de artículos como el *Systematic Literature Review*. Los resultados y conclusiones obtenidas ubican a las redes MANET y VANET como temas motores en la propuesta de soluciones de seguridad durante los últimos 10 años. Además, si bien abundan las soluciones de detección de ataques o intrusiones, existe cierta confusión a la hora de enmarcar dichas soluciones por líneas de defensa. Es por lo anterior, por lo que se propone una taxonomía extendida que, desde nuestro punto de vista, mejora la clasificación tradicional añadiendo nuevas líneas de defensa como la tolerancia.

***Index Terms*—*ad hoc*, Seguridad, Resiliencia, Tolerancia, MANET, VANET**

I. Introducción

Una red ad hoc es una red descentralizada, que no utiliza ninguna infraestructura subyacente, muy flexible y con un despliegue rápido. Sin embargo, las características intrínsecas de este tipo de redes hacen que sean objeto de multitud de ataques de seguridad, con distintos propósitos.

De entre la amalgama de ataques existentes en este tipo de redes [1], destacar aquellos pertenecientes a la familia de *packet dropping*, que consisten en descartar información deliberadamente. Otros ejemplos son, *jamming*, que provoca denegación de servicio principalmente a nivel físico o *eavesdropping*, que trata de interceptar información de manera no autorizada.

Motivado por todo lo anterior, se presenta un estudio pormenorizado y metodológico del estado de la Literatura para la seguridad en redes ad hoc. Para ello, utilizaremos técnicas y métodos derivados del análisis bibliométrico y del Systematic Literature Review (SLR). A través del análisis bibliométrico, principalmente con *Science Mapping* [2]), se obtendrán las tendencias y tecnologías motoras en el contexto del trabajo. Por otro lado, y a partir de los resultados anteriores, se procederá a estudiar en profundidad aquellos trabajos relacionados con los temas motores obtenidos anteriormente siguiendo una metodología SLR (Kitchenham, B. *et al.* [3] y [4]).

Tras la aplicación de las metodologías anteriores, se concluye que la seguridad en redes ad hoc es todavía un tema de discusión, sobre todo en Mobile Ad hoc Networks (MANETs) y Vehicular Ad hoc Networks (VANETs), y que la mayoría de las soluciones de seguridad se centran en la familia de ataques *packet dropping* así como en protocolos específicos de *routing* como Ad hoc On-Demand Distance Vector (AODV) [5].

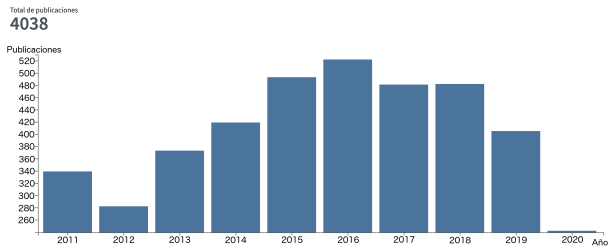
Además, después de analizar una serie de revisiones del estado del arte publicadas en la última década, se pueden encontrar muchas clasificaciones diferentes para una variedad de propósitos, p. ej. por ataques específicos [6], [7], por tipo de Intrusion Detection System (IDS) [8], [9], por *Line-of-Defense* (LoD) [10], etc. Sin embargo, no hemos encontrado una clasificación adecuada de las propuestas de seguridad actuales para redes ad hoc por LoD. Por eso, este trabajo propone una actualización de la taxonomía clásica. Con la adición de nuevas LoD como la **Tolerancia** donde se enmarcan aquellas soluciones que intentan mitigar los efectos del ataque sin necesidad de conocer su existencia ni actuar directamente contra él.

El resto del documento se estructura como sigue. En la Sección II se realiza un estudio bibliométrico y mapeo de la Literatura (*Science Mapping*) para obtener un análisis de tendencias en seguridad en redes ad hoc. Los resultados obtenidos son utilizados en la Sección III, para realizar un SLR sobre redes VANETs y MANETs. En la Sección IV, se presenta y describe la nueva taxonomía propuesta que trata de solventar la falta de consenso y homogeneización en lo que respecta a las líneas de defensa. Para finalizar, en la Sección V se resumen las principales conclusiones extraídas.

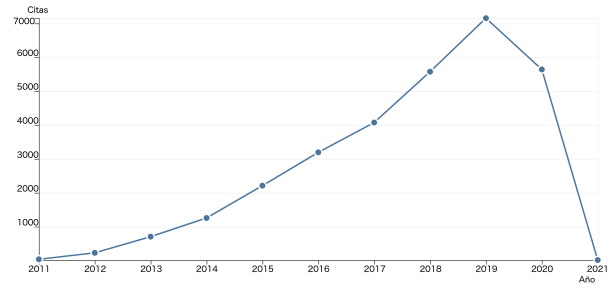
II. Estudio bibliométrico y análisis de temáticas, tendencias y evolución en la seguridad en redes ad hoc

En bibliometría, se utilizan principalmente dos técnicas: Análisis de Rendimiento y *Science Mapping* [11] [12]. 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. 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.

La base de datos utilizada para realizar el estudio bibliométrico es la *Web of Science* (WoS). Para seleccionar el conjunto de documentos se ha realizado una búsqueda



(a) Documentos por año de publicación.



(b) Citas por año de publicación.

Figura 1. Informes de documentos y citas de la WoS (Octubre de 2020)

metodológica por palabras clave sobre el tema con consultas como la del ejemplo a continuación:

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

En esta consulta, TS busca términos en los campos "Título", "Abstract", "Palabras clave de autor" y "KeyWords Plus". Mientras que SU hace lo propio en el campo "Áreas de investigación". Esta consulta devolvió unos 4000 resultados entre los años 2011 y 2020. Los primeros datos relevantes extraídos de los informes de citas y publicaciones de la WoS (ver Figura 1) se comentan a continuación. En la Figura 1(a) se observa un informe de documentos publicados por año en la última década, mientras que en la Figura 1(b) se puede ver un informe del número de citas por año. 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 partir de la búsqueda anterior, se obtuvieron los meta datos de todos los documentos que devolvió la base de datos en forma de *dataset* en texto plano. A continuación, siguiendo la metodología de Cobo, M.J. *et al.* [2], se realizó un exhaustivo análisis bibliométrico con ayuda del software SciMAT [13]. De este análisis resultan los llamados diagramas estratégicos y redes temáticas. Los primeros sitúan las temáticas según la tendencia detectada, usando dos parámetros: centralidad y densidad, ambas definidas por Callon *et al.* [14].

Los mapas de redes temáticas agrupan los temas relacionados con la temática principal, situándose en el centro del cluster el tema más central, dando nombre al cluster y a la temática detectada. La forma de interpretar el diagrama estratégico y la relevancia del tema se hace en función del cuadrante en donde se localiza:

Cuadrante superior derecho: temas bien desarrollados y de importancia dentro del campo de estudio. Son temas motores de la especialidad. **Cuadrante superior izquierdo:** temas con fuerte cohesión interna, pero débil interconexión externa. Temáticas muy concretas y especializadas. **Cuadrante inferior derecho:** temas poco desarrollados internamente y sin embargo con una fuerte interconexión externa. Podrían ser temas transversales. **Cuadrante inferior izquierdo:** temas poco desarrollados tanto interna como externamente. en este caso tenemos dos posibilidades, bien pueden ser temas emergentes, o temas en declive o desaparecidos.

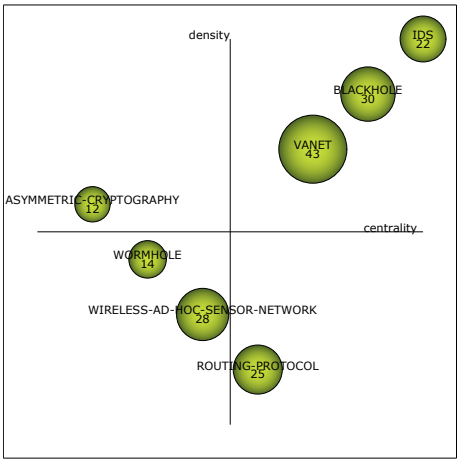


Figura 2. Diagrama estratégico para el Índice-h. Subperiodo 2011 - 2015.

Tabla I
MEDIDAS DE RENDIMIENTO DE LOS GRUPOS DEL SUBPERIODO 2011 - 2015.

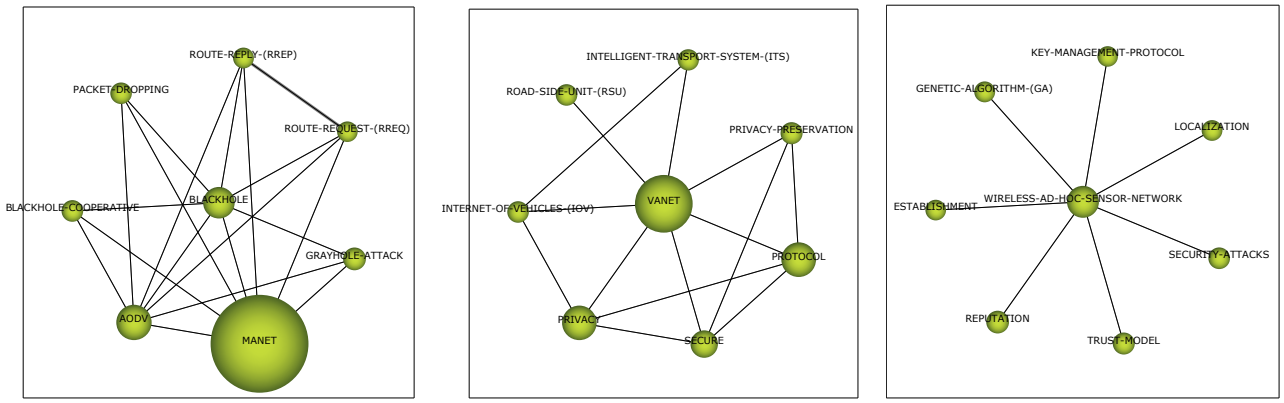
Nombre del tema	Número de documentos	Índice-h ▽	Promedio de citas	Número de citas
VANET	486	43	14, 85	7,215
Blackhole	719	30	5, 83	4,194
Wireless Ad Hoc Sensor Network	164	28	20, 76	3,405
Routing Protocol	304	25	9, 36	2,845
IDS	138	22	14, 69	2,027
Wormhole	141	14	7, 3	1,029
Asymmetric Criyptography	70	12	5, 36	375

Haciendo uso de estos diagramas, se ha realizado un mapeo del estado conceptual de la seguridad en redes ad hoc, detectando las áreas temáticas en las que más tarde centrar la revisión sistemática de la Literatura. El análisis se divide en dos subperiodos: desde 2011 a 2015 y desde 2016 a 2020, con objeto de analizar la evolución de las temáticas a lo largo de los años. Los resultados se muestran y analizan a continuación.

II-A. Análisis del subperiodo 2011 - 2015

En la Figura 2 se observa el diagrama estratégico para el *índice-h* de los documentos correspondientes al primer subperiodo (la cifra dentro de las esferas es el *índice-h* de esa temática en ese subperiodo).

Según la disposición observada en el diagrama estratégico y los datos correspondientes presentados en la Tabla I, aparecen como temáticas motor: VANET, *Blackhole* e IDS. Además, se aprecia que el concepto general *redes de sensores ad hoc* se ubica en el cuarto cuadrante, sin embargo obtiene un *índice-h*



(a) Temática *Blackhole* (b) Temática VANET (c) Temática *Wireles Ad hoc*

Figura 3. Redes temáticas del subperiodo2011 - 2015.

elevado. Estos temas del primer subperiodo tienen un alto número de citas, sobre todo VANET y *Blackhole*, con un *indice-h* alto, que los corrobora como temas motor. En cuanto a IDS, se trata de una temática con una situación particular, debido a su posterior absorción por MANET en el siguiente subperiodo. En lo que respecta a las redes temáticas las más relevantes se muestran en la Figura 3. La elección de dichas redes viene dada por su posición en las tablas de rendimiento (Tablas I y II), ordenadas por la columna para el *índice-h* de manera descendente.

Dentro de la temática *Blackhole* (Figura 3(a)) aparece de manera muy relevante el tema MANET, relacionándose con temas del que parece haber sido el punto débil de este tipo de redes *ad hoc* durante esos años, el ataque de *packet dropping*, así como con el protocolo de enrutamiento clásico de MANETs, el AODV. Configurando una temática en común. Esto pone de manifiesto el esfuerzo por parte de la comunidad investigadora en sofocar esta amenaza principalmente en el contexto de las MANETs.

En la red temática de VANET (Figura 3(b)) se observa que se relaciona con temas de privacidad y seguridad en los protocolos, y se establece una conexión única entre VANETs y Road Side Unit (RSU), que muestra su dependencia.

Wireles Ad hoc Sensor Network (Figura 3(c)), con un Índice-h elevado a pesar del escaso número de documentos, se perfila como tema transversal, como se verá en el siguiente subperiodo, apareciendo junto a términos dispares que no se relacionan entre sí.

II-B. Análisis del subperiodo 2016 - 2020

En la Figura 4 se observa el diagrama estratégico del segundo subperiodo para el *indice-h* de los documentos. Según dicha figura, y las medidas mostradas en la Tabla II, se aprecia como VANET se ha colocado en una posición de centralidad absoluta en los últimos 5 años. Mientras que MANET ha tomado el centro de su temática (cluster), y ambas temáticas se postulan como temas motor. Aparece en este subperiodo un nuevo tema motor *Physical Layer Security*, con un número de documentos pequeño, pero con un promedio de citas relativamente alto que resulta llamativo.

En lo que respecta a las redes temáticas de este subperiodo (Figura 5) para los temas más relevantes, en la Figura 5(a) se observa como VANET sigue ocupando su posición

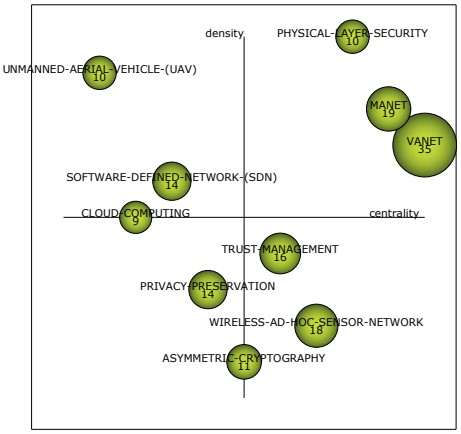
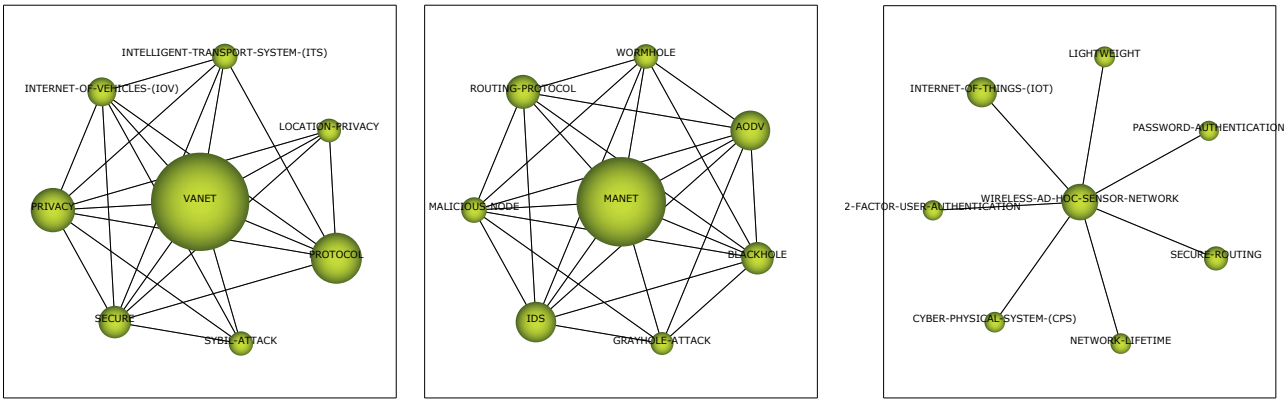


Figura 4. Diagrama estratégico para el Índice-h. Subperiodo 2016 - 2020.

Tabla II
MEDIDAS DE RENDIMIENTO DE LOS GRUPOS DEL SUBPERIODO 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
Unmaned Aerial Vehicle (UAV)	38	10	17, 45	663
Cloud Computing	53	9	7, 25	384

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) (Kaiwartya, O. *et al.* [15]). También se puede ver que aparece el *Sybil Attack* como posible punto débil afectando a la privacidad



(a) Temática VANETs (b) Temática MANETs (c) Temática *Wireles Ad hoc*

Figura 5. Redes temáticas del subperiodo 2016 - 2020.

de los vehículos conectados. Un ataque *Sybil Attack* ocurre cuando un sistema distribuido es corrompido por una única entidad que controla distintas identidades de dicho sistema.

En cuanto a MANET (Figura 5(b)), sigue teniendo su propio punto débil, el ataque de *packet dropping* (representado por temas como *Blackhole*, *Grayhole attack* y *Wormhole*) afectando a su principal protocolo de routing AODV. Otro detalle de este cluster es que integra a IDS, esta temática del subperiodo 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 MANETs.

Wireless Ad hoc Sensor Network (Figura 5(c)) 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, queremos destacar *Internet Of Things* (IoT): definición comercial del concepto de *interconexiones de dispositivos electrónicos cotidianos*, que puede o no basarse en redes ad hoc. Por la referencia al paradigma general donde se sitúa la problemática que se está estudiando. Y Cyber-Physical System (CPS): un sistema ciberfísico, según el Dr. Edward A. Lee [16], son integraciones de computación y procesos físicos. Por la cercanía al caso de estudio de las redes VANETs, donde, por ejemplo, un CPS hace referencia a los vehículos autónomos en el contexto de estas redes ad hoc.

III. Estado actual de la Literatura: revisión sistemática

Antes de entrar en materia, en relación a las líneas de defensa tradicionalmente se diferencia entre tres [17]:

- **Prevención.** En esta línea se agrupan los mecanismos de seguridad que tratan de prevenir ataques.
- **Detección.** Son mecanismos de detección aquellos destinados a identificar actividades inadecuadas, incorrectas o anómalas dentro de las redes o sistemas bajo monitorización.
- **Respuesta.** Una vez detectado el ataque, reaccionaran respondiendo a la amenaza los mecanismos de respuesta.

A partir del estudio bibliométrico de la seguridad en redes ad hoc realizado en la seccion anterior se han extraído las principales temáticas y tendencias en investigación. Más aún, ha quedado patente que actualmente es un tema que atrae la atención de la comunidad investigadora, sobre todo en MANETs y VANETs. Así, la revisión sistemática de la Literatura que se presenta a continuación se ha centrado en estas dos temáticas específicas.

Como parte inicial de la metodología de Kitchenham *et al.* [3] se han planteado las siguientes cuestiones de investigación a resolver en este análisis:

Cuestión 1: ¿En que líneas de defensa se ha centrado la investigación en redes ad hoc?

Cuestión 2: ¿Existe confusión en la clasificación por LoD?

Cuestión 3: ¿Es necesaria la propuesta de nuevas taxonomías?

Siguiendo la metodología de Kitchenham, los criterios de selección de estudios están destinados a identificar aquellos estudios primarios[1] que proporcionan evidencia directa una pregunta de investigación específica. En el caso del presente trabajo, se han usado las cuestiones de investigación tanto para la selección de estudios primarios como secundarios[2]. Para más información sobre el significado de estudio primario y secundario se remite al lector a consultar el trabajo de Kitchenham *et al.* [3]. Se debe tener en cuenta que se han leído y revisado más de 100 referencias entre estudios primarios y secundarios. Sin embargo, aquí nos centramos en las conclusiones extraídas.

Como primer paso, se extrajeron y analizaron un conjunto de trabajos pertenecientes a los últimos 10 años que abordan la seguridad en redes ad hoc. Dicha revisión se sintetiza en la Tabla III, en la que se pueden ver los tipos de ataques cubiertos; si los autores realizan alguna clasificación de soluciones en algún sentido; y los tipos de soluciones propuestas. La cantidad de *Surveys* en los que hemos encontrado estas pautas se muestra en porcentaje. Como bien se observa en la comentada Tabla III, son pocos los autores que clasifican por LoD. También se observa que los autores continúan

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

[2]Estudio secundario. Un trabajo que revisa todos los estudios primarios posibles, con el objetivo de integrar/sintetizar evidencia relacionada con una o varias preguntas de investigación.

Tabla III
CONCLUSIONES EXTRAÍDAS DE LOS SURVEYS ANALIZADOS.

Ataques cubiertos	# (%) ▽	Clasificación	# (%) ▽	Conclusión	# (%) ▽
Varios	47 %	Tipologías de ataques	18 %	Trust	29.4 %
Packet Dropping	24 %	Gestión de trust	17.65 %	Cryptographic	18 %
-	18 %	-	17.65 %	Resilience	17.6 %
Modification	6 %	Requisitos de VANET	11.76 %	IDS	11.8 %
Information attack	6 %	Tecnologías y aplicación de VANET	11.76 %	Multilayer	6 %
		IDSs	11.76 %	Bio-inspired	5.9 %
		Algoritmos Bio-inspirados	5.88 %	Notification	5.9 %
		Soluciones resilientes	5.88 %		
		Líneas de defensa	5.88 %		

Tabla IV
RESUMEN DE LAS BÚSQUEDAS EN LAS DISTINTAS BIBLIOTECAS.

	TOTAL	P	D	R	P∩D	P∩R	D∩R	P∩D ∩R
Springer	3285	123	912	675	66	13	262	117
ACM	710	38	79	20	21	5	11	46
Scopus	14606	1081	5231	720	791	20	272	354
IEEE	3949	19	115	17	8	0	1	7
WoS	157	50	327	25	22	0	9	0
Average		**262**	**1331**	**291**	**182**	**8**	**111**	**105**

proponiendo soluciones basadas principalmente en técnicas de criptografía y confianza.

A través de la Tabla III podemos concluir que son pocos los trabajos que abordan la clasificación de LoD. También se observa que los autores siguen proponiendo soluciones basadas principalmente en técnicas de criptografía y confianza. Un estudio en profundidad de los estudios secundarios que proponen una clasificación de LoD (normalmente basados en las líneas de defensa clásicas: prevención, detección y respuesta/-reacción [10]) y los estudios primarios referenciados, muestra que la mayoría de ellos no se pueden situar unívocamente en una línea de defensa. Por ejemplo, en [18] los autores hablan de detectar y prevenir, pero lo que realmente hacen es detectar y responder; o en [19] los autores evitan llamar a su solución por detección, la llaman evitación de intrusiones. Y un tercer ejemplo, el trabajo de Pandey, S. [20] trata sobre detección del ataque *Blackhole* con técnicas de *Machine Learning*, sin embargo, también aportan una respuesta. Es más, algunas soluciones no encajan en absoluto en ninguna de las clásicas LoD y otras fueron simplemente mal clasificadas por los autores.

Por ello, se realiza una búsqueda sistemática en las bibliotecas digitales más relevantes. Con el fin de corroborar empíricamente la búsqueda de soluciones de prevención, detección y respuesta. Por ello, se han realizado consultas complejas como la siguiente:

```
(TS = (security networks ''ad ho'') AND
TS = (manet OR vanet) AND TS = (preve-
ntion AND detection) NOT TS = (respon-
se) AND SU = (Engineering OR Computer
Science))
```

Esta consulta particular corresponde a la columna de búsqueda P∩D en la WoS de la Tabla IV, que resume los resultados obtenidos mientras que la Figura 6 los representa. A través de la Tabla IV, se muestra el número de artículos que centran las palabras clave prevención (P), detección (D) y respuesta (R). Además, también se buscan conjuntos de artículos que se solapan, es decir, conjuntos de artículos con diferentes combinaciones de estas palabras clave. En la Figura 6 se representa gráficamente el solapamiento existente entre las soluciones a partir de los valores promediados.

Del estudio anterior podemos concluir que no existe un consenso único en la comunidad investigadora sobre lo que significa la prevención, la detección y la respuesta. En consecuencia, es muy difícil clasificar las soluciones de seguridad en redes y sistemas en general y en redes ad hoc en particular.

Además, recientemente nos hemos dado cuenta de que, como ya se ha comentado, algunas soluciones no encajan en absoluto en ninguna de las clásicas LoD. Por ello, podría ser necesario definir nuevas líneas de defensa como la introducida por Magán-Carrión en [21]: la tolerancia. Las soluciones tolerantes son aquellas ideadas para preservar los servicios para los que fue diseñado el sistema en presencia de ataques. En relación con las soluciones de tolerancia, las propuestas de supervivencia pueden ser vistas como tolerantes, tal y como se describe en [22].

Además de las anteriores LoD tradicionales, aquí incluimos otra más: la tolerancia. Esta LoD abarca todos los estadíos temporales de un ataque y no pretende a priori, mitigar los efectos del ataque sino tolerarlo. Como ya mencionaron Magán-Carrión *et al.* [1], haciendo referencia a la supervivencia 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 [23].

Los datos mostrados hasta ahora reflejan que una gran parte del esfuerzo se ha volcado en la de detección. Lo que responde a la cuestión 1. Además se aprecia la dificultad para separar completamente la clasificación de soluciones por LoD tradicionales, y la necesidad de trabajos como el presente, que realicen una meticulosa revisión de la Literatura para comprender toda esta problemática. Lo que responde a las cuestiones 2 y 3. Por lo tanto, teniendo en cuenta lo descrito hasta ahora, queda clara la necesidad de una nueva clasificación por LoD que recoja de forma mas concreta el tipo exacto de las soluciones de seguridad existentes, mejorando así la actual clasificación.

IV. TAXONOMÍA EXTENDIDA POR LÍNEA DE DEFENSA

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).

- **Prevención:** Aquellas soluciones que tratan de evitar el ataque, por lo que actúan antes del ataque.
- **Detección:** Soluciones que detectan el ataque, por lo que actúan después del ataque, es decir, no lo evitan.

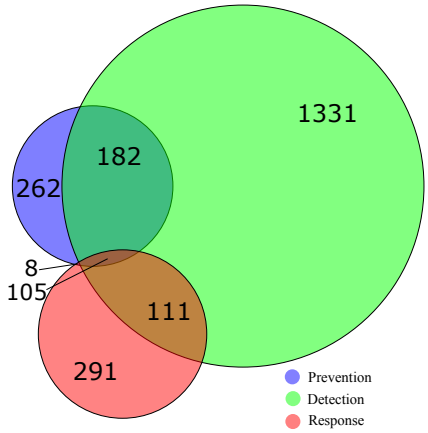


Figura 6. Agrupación según líneas de defensa. Modelo tradicional.

Se clasifican las soluciones que realicen una detección pura, sin ninguna reacción en contra.

- **Detección + Reacción:** Esta sección engloba aquellas soluciones que detectan el ataque y además realizan alguna labor de respuesta.
- **Tolerancia:** Soluciones que no evitan el ataque, sino que tratan de mitigar los efectos negativos que afecten a los servicios y rendimiento de la red, en lugar de realizar acciones de bloqueo.

Con este nuevo enfoque se pretende recategorizar y reordenar las soluciones encontradas y estructurar una nueva taxonomía por líneas de defensa. 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.* [1] concluyeron, se necesitan soluciones que actúen en todas las líneas de defensa, y que además sean capaces de tolerar el ataque.

Además de 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.

V. Conclusiones

A pesar de sus especiales características, las redes ad hoc adolecen de diferentes debilidades desde el punto de vista de la seguridad. A lo largo del presente trabajo se pone de manifiesto la relevancia y preocupación actual en este aspecto, en concreto y específicamente en MANETs y VANETs. Además, es notable la confusión existente en la clasificación de soluciones de seguridad en este tipo de redes en función de la línea de defensa. Motivados por lo anterior, destacar la propuesta de una taxonomía que primero, ayudará a la clasificación de soluciones en esta línea y segundo pretende guiar, en cierto sentido, la actuación y propuesta futuras de soluciones de seguridad por línea de defensa por parte de la comunidad investigadora.

Referencias

[1] R. Magan-Carrion, "Supervivencia en redes ad hoc. Mecanismos de tolerancia y reacción frente amenazas de seguridad." Ph.D. dissertation, Universidad de Granada, 2016.
[2] M. Cobo, "An approach for detecting, quantifying, and visualizing the evolution of a research field: A practical application to the Fuzzy Sets Theory field," *Journal of Informetrics*, vol. 5, no. 1, pp. 146–166, 2011.
[3] B. Kitchenham, "Procedures for performing systematic reviews," *Keele University,UK and National ICT Australia*, vol. 33, no. 2004, pp. 1–28, 2004.
[4] B. Kitchenham and S. M. Charters, "Guidelines for performing systematic literature reviews in software engineering," Keele University, Tech. Rep., 2007.
[5] C. E. Perkins, "Ad-hoc on-demand distance vector routing," in *Proceedings - WMCSA'99: 2nd IEEE Workshop on Mobile Computing Systems and Applications*, 1999, pp. 90–100.
[6] S. Zeadally, "Vehicular ad hoc networks (VANETS): status, results, and challenges," *Telecommunication Systems*, vol. 50, no. 4, pp. 217–241, aug 2012.
[7] A. Sardana, T. Bedwal, A. Saini, and R. Tayal, "Black hole attack's effect mobile ad-hoc networks (MANET)," in *2015 International Conference on Advances in Computer Engineering and Applications*. IEEE, mar 2015, pp. 966–970.
[8] A. Saxena, "A review on intrusion detection system in mobile ad-hoc network," in *2017 International Conference on Recent Innovations in Signal processing and Embedded Systems (RISE)*, vol. 2018-Janua. IEEE, oct 2017, pp. 549–554.
[9] N. Khanna, "A comprehensive taxonomy of schemes to detect and mitigate blackhole attack and its variants in MANETs," *Computer Science Review*, vol. 32, pp. 24–44, may 2019.
[10] A. Ghosal and M. Conti, "Security issues and challenges in V2X: A Survey," *Computer Networks*, vol. 169, p. 107093, mar 2020.
[11] E. Noyons, "Combining mapping and citation analysis for evaluative bibliometric purposes: A bibliometric study," *Journal of the American Society for Information Science*, vol. 50, no. 2, pp. 115–131, 1999.
[12] A. F. Van Raan, "Measuring Science," in *Handbook of Quantitative Science and Technology Research*. Dordrecht: Springer Netherlands, 2004, pp. 19–50.
[13] M. Cobo, "SciMAT: A new science mapping analysis software tool," *Journal of the American Society for Information Science and Technology*, vol. 63, no. 8, pp. 1609–1630, 2012.
[14] M. Callon, "Co-word analysis as a tool for describing the network of interactions between basic and technological research: The case of polymer chemsitry," *Scientometrics*, vol. 22, no. 1, pp. 155–205, 1991.
[15] O. Kaiwartya, "Internet of Vehicles: Motivation, Layered Architecture, Network Model, Challenges, and Future Aspects," *IEEE Access*, vol. 4, pp. 5356–5373, 2016.
[16] E. A. Lee, "Cyber physical systems: Design challenges," EECS Department, University of California, Berkeley, Tech. Rep. UCB/EECS-2008-8, 2008.
[17] P. García Teodoro, *Seguridad en redes y sistemas de comunicación: teoría y práctica*. Independently Published, 2020.
[18] A. Ansari, "Flooding attack detection and prevention in MANET based on cross layer link quality assessment," in *2017 International Conference on Intelligent Computing and Control Systems (ICICCS)*, vol. 2018-Janua. IEEE, 2017, pp. 612–617.
[19] E. Elmahdi, "Secure and reliable data forwarding using homomorphic encryption against blackhole attacks in mobile ad hoc networks," *Journal of Information Security and Applications*, vol. 51, p. 102425, apr 2020.
[20] S. Pandey and V. Singh, "Blackhole Attack Detection Using Machine Learning Approach on MANET," in *2020 International Conference on Electronics and Sustainable Communication Systems (ICESC)*. IEEE, jul 2020, pp. 797–802.
[21] R. Magán-Carrión, "Seguridad para la supervivencia en redes ad hoc," in *Supervivencia en redes ad hoc. Mecanismos de tolerancia y reacción frente amenazas de seguridad.* Universidad de Granada, 2016, ch. 2, pp. 17 – 39.
[22] M. N. Lima, "A survey of survivability in mobile Ad hoc Networks," *IEEE Communications Surveys and Tutorials*, vol. 11, no. 1, pp. 66–77, 2009.
[23] Ponemon Institute, "2018 cost of a data breach study: Global overview," *IBM Security Services*, no. July, p. 76, 2018.