TELEMÁTICA
REVISTA DIGITAL de las Tecnologías de la Información y las Telecomunicaciones
Revista Telemática. Vol.20 No.3 , Julio-Septiembre, 2021, p.49- 60 ISSN 1729-3804

ANÁLISIS DEL COMPORTAMIENTO DE LAS REDES MALLADAS INALÁMBRICAS BAJO LA INFLUENCIA DE ATAQUES DE DENEGACIÓN DE SERVICIOS

Damian O. Ruiz Varona[1], Anays Guilarte Acosta[2], Walter Baluja Garcia[3]

[1,2]Universidad Tecnológica de la Habana "José Antonio Echeverría", CUJAE, Ave. Independencia No.34515, Km 14½,Reparto 1ro de Mayo, Boyeros, La Habana, Cuba. ; [3]Universidad de las Ciencias Informáticas, UCI, Carretera a San Antonio de los Baños, Km 2 ½, reparto Torrens, municipio Boyeros, La Habana, Cuba.

[1]e-mail:damianrvaro@gmail.com
[2]e-mail:anyacosta94@gmail.com
[3]e-mail:walterb@uci.cu

RESUMEN

Las Redes Malladas Inalámbricas (WMNs por sus siglas en Inglés) son redes de datos con topología de malla, formadas por nodos que establecen y mantienen la conectividad de red automáticamente. Son auto-configurables, y fácilmente adaptables a diferentes necesidades de tráfico y cambios de la red. A pesar de estas ventajas, presentan vulnerabilidades en cuanto a la seguridad y son propensas a diferentes ataques, entre los que se destacan los de Denegación de Servicios (DoS, por sus siglas en inglés). A pesar de que en Cuba este tipo de redes no están desplegadas, sí existen diversos escenarios rurales y urbanos donde su aplicación resolvería de una manera económica y eficaz, las carencias de conectividad y de acceso a los servicios de datos. Por tales motivos, este trabajo da continuidad al estudio sobre la seguridad en las redes inalámbricas basadas en los estándares 802.11. En este caso se analizaron ataques que tienen como objetivo la DoS en la Capa de Enlace de Datos y la Capa de Red del modelo de Interconexión de Sistemas Abiertos (OSI, por sus siglas en inglés). La herramienta utilizada para la simulación de los escenarios fue OMNET++ y módulos de los *frameworks* INET y NETA. Las mediciones se realizaron sobre el *throughput*, el porciento de paquetes perdidos y los cambios en la topología de la red. Los resultados obtenidos pueden influir en importantes decisiones del despliegue de las WMN, tales como la topología de red y el protocolo de enrutamiento empleados, entre otros.

PALABRAS CLAVES: Redes Malladas Inalámbricas, seguridad, ataques, denegación de servicios.

BEHAVIOR ANALYSIS OF WIRELESS MESH NETWORKS UNDER DENIAL OF SERVICES ATTACKS

ABSTRACT

Wireless Mesh Networks (WMNs) are data networks with mesh topology, formed by nodes that establish and maintain network connectivity automatically. They are self-configuring and easily adaptable to different traffic needs and network changes. Despite these advantages, they have security vulnerabilities and are prone to different attacks, including Denial of Service (DoS) attacks. Although in Cuba this type of network is not deployed, there are several rural and urban scenarios where their application would solve economically and effectively, the lack of connectivity and access to data services. For these reasons, this work gives continuity to the study on security in wireless networks based on 802.11 standards. In this case, attacks targeting the DoS in the Data Link Layer and the Network Layer of the OSI model were analyzed. The tool used for the simulation of the scenarios was OMNET++ along with modules from the INET and NETA frameworks. The measurements were made on the throughput, the percentage of lost packets, and the changes in the network topology. The results obtained can influence important decisions in the deployment of WMNs, such as the network topology and the routing protocol used, among others.

INDEX TERMS: WMN, security, attacks, DoS.

1. INTRODUCCIÓN

Las Redes Inalámbricas están formadas por estaciones que no están conectadas por cables o fibras, pero que pueden comunicarse a través de otros medios, como señales de radio y luces infrarrojas [1]. La tecnología inalámbrica ofrece

Manuscrito recibido:11-11-2020, aceptado: 23-11-2020
Sitio web:http://revistatelematica.cujae.edu.cu/index.php/tele

robustez, provisionalidad y movilidad (aunque limitada en una determinada área). Las Redes Malladas Inalámbricas han emergido como una tecnología esencial de las redes inalámbricas [2]. Pueden desplegarse rápidamente sin necesidad de utilizar cables ni importantes soportes de infraestructura [3].

Una WMN consiste en clientes y *routers* interconectados en malla, donde generalmente los *routers* forman una infraestructura de *backbone* inalámbrico que se interconecta con redes cableadas para ofrecer a los clientes una conexión multi-saltos hacia Internet [4]. Los componentes que forman la arquitectura de *backbone*, como las estaciones bases y los puntos de acceso, son también llamados *mesh routers*. Estos tienen poca movilidad y energía ilimitada. Los *mesh routers* con funcionalidades de *gateway* permiten la integración de redes existentes y la conexión a Internet. Por lo general, las WMNs son usadas como redes de transporte, por lo que suelen estar conectados a una red externa.

Las WMNs proporcionan una solución barata, rápida y eficaz para las redes inalámbricas de datos en zonas urbanas, suburbanas y en los entornos rurales [5]. El despliegue de las redes inalámbricas institucionales y comunitarias en Cuba propicia que las WMNs se conviertan en una de las alternativas de solución para el acceso a los servicios por parte de los usuarios, teniendo en cuenta el bajo costo de su instalación y de mantenimiento. Por otra parte, en el país no se encuentran trabajos que integren el entorno de simulación de OMNET y *frameworks* como NETA con el propósito de abordar el tema de la seguridad en WMNs. Por tanto, este trabajo posee una marcada relevancia científica en la realidad cubana actual, en torno al despliegue de nuevas facilidades para la interconexión de usuarios y creación de nuevos servicios.

Las WMNs poseen varias vulnerabilidades de seguridad y son objeto de diversos ataques debido, fundamentalmente, a la naturaleza descentralizada y a la comunicación multi-salto a través de nodos intermediarios. La fuente de los ataques puede ser tanto externa como interna. En el caso de los ataques externos, un cliente no autorizado puede "escuchar" de forma pasiva sobre el canal, comprometiendo la confidencialidad de la información, o bien dañar la disponibilidad del canal, interfiriendo en el intercambio de datos entre los nodos de la red. Los ataques internos son lanzados desde nodos integrantes de la red considerados "maliciosos", los cuales violan las reglas de los protocolos de enrutamiento y degradan el rendimiento general de la red [6].

A pesar de su auge y desarrollo, el reto técnico en cuanto a la seguridad en el despliegue de WMN no ha sido resuelto. Pese a todos los esquemas de seguridad que han sido propuestos para las Redes Inalámbricas de Área Local (WLANs, por sus siglas en inglés) en los últimos años, no hay ninguno que solucione todos los problemas de las WMNs [3]. Varios proyectos [7] [8] [9] [10] han enfatizado la importancia del equilibrio entre seguridad y desempeño en redes inalámbricas multi-saltos.

Los ataques DoS son una de las grandes amenazas sobre las WMNs y su estudio se amplía cada vez más debido a que son muy comunes. Algunos servicios de la red, como el enrutamiento, pueden verse afectados como consecuencia de estos ataques. Por tal motivo, múltiples investigaciones se han enfocado en analizar y proponer soluciones que minimicen el impacto de las posibles amenazas y le proporcionen a la red ciertos índices de garantía de calidad y, consecuentemente, una mejora de la experiencia del usuario.

Los problemas de seguridad pueden dar al traste con la Calidad de Servicio (QoS, por sus siglas en inglés) [7]. Por consiguiente, garantizar la calidad aún bajo la influencia de ataques a la red es un objetivo de interés. Por tales motivos, el presente trabajo se propone analizar los efectos más importantes que tienen algunos ataques DoS sobre las WMNs a partir del diseño e implementación de varios escenarios de simulación y, la recopilación y procesamiento de datos de simulación.

2. SIMULACIÓN DE ATAQUES A LAS WMN Y ANÁLISIS DE LOS RESULTADOS

En general los trabajos científicos donde se hace uso de simuladores para redes de datos, no incluyen *framework*s ni extensiones de seguridad que permitan la implementación de dichos escenarios. Por su parte, OMNET++ [https://omnetpp.org/] es una solución muy utilizada en el ámbito académico porque permite examinar la marcha de las simulaciones en tiempo real mediante la sucesión de eventos discretos. Esta herramienta permite la utilización de un *framework* que facilita la simulación de eventos o ataques de seguridad. En este trabajo se emplearon INET [https://inet.omnetpp.org/] y NETA [http://nesg.ugr.es/index.php/en/neta], librerías que se basan en los mismos principios que OMNET++, módulos que se comunican entre sí mediante el intercambio de mensajes. INET contiene los dispositivos, protocolos y modelos de red necesarios para la simulación, mientras que NETA tiene implementado algunos ataques de seguridad. Para el diseño de los escenarios y la implementación de los ataques, se utilizaron OMNETv5.0, INETv3.4 y NETAv1.0.

TELEMÁTICA
REVISTA DIGITAL de las Tecnologías de la Información y las Telecomunicaciones
Revista Telemática. Vol.20 No.3 , Julio-Septiembre, 2021, p.49-60 ISSN 1729-3804

Los ataques simulados estuvieron dirigidos a la Capa de Enlace y la Capa de Red del modelo OSI. En la simulación los nodos atacantes aprovechan las debilidades del protocolo de Capa de Enlace MAC IEEE802.11[11] mediante los ataques *MACJamming* y *Flooding*. Por otra parte, para la Capa de Red, se simularon ataques al enrutamiento del tipo *Sinkhole* y *Grayhole*. En todos los casos se empleó una topología de infraestructura[12], similar a la representada en la Fig. 1. El medio inalámbrico seleccionado tiene características ideales, garantizando la simplicidad y la rapidez en la simulación. Esto quiere decir que el éxito en la recepción solo va a depender del rango de transmisión, el rango de interferencia y el rango de detección de los nodos.

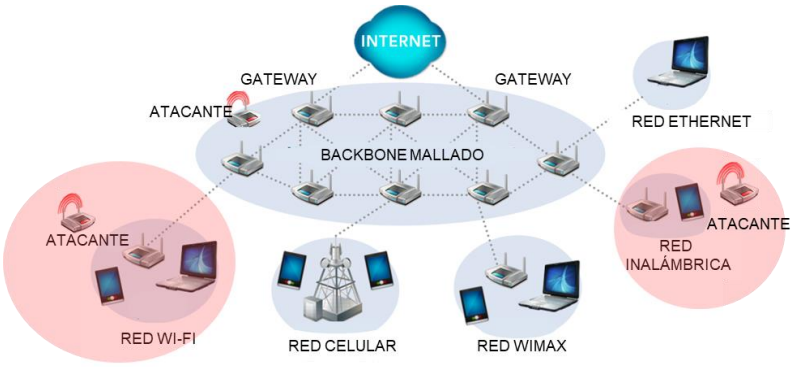

Figura 1: Modelo de topología de Infraestructura.

Ataques DoS a la Capa de Enlace

Fueron simulados ataques. Los resultados se analizaron a partir del fichero .anf, generado automáticamente al finalizar la simulación. Los parámetros a medir fueron: la relación entre paquetes transmitidos y recibidos, y el rendimiento de la red a través del *throughput*. En este punto se considera irrelevante la utilización de diferentes protocolos de enrutamiento, por tanto, los escenarios descritos a continuación utilizarán siempre AODV (*Ad hoc On demand Distance Vector*) para el descubrimiento de las rutas.

Escenario1. Ataque MACJamming: *Jamming* se define como el acto de dirigir intencionalmente señal electromagnética hacia un sistema de comunicación para interrumpir o prevenir la transmisión. El ataque *Jamming* puede ser visto como un caso especial de DoS [13]. En el ataque *MACJamming*, el objetivo del nodo atacante consiste en interrumpir la comunicación entre los nodos de la red mediante la emisión de una señal interferente. El nodo atacante aprovechará las debilidades del protocolo de nivel 2, MAC IEEE802.11, y del algoritmo de acceso al medio, Acceso Múltiple por Detección de Portadora y Prevención de Colisiones [14]. Los aspectos vulnerables que se aprovechan son el mecanismo de temporización y el intercambio de las tramas de control RTS/CTS (*Request to Send*/*Clear to Send*), asumiendo que todos los nodos trabajan con estas especificaciones.

Las variables establecidas por los autores para controlar el ataque fueron la activación (*activeAttack*) y el tipo de ataque (*attackType*), que para este caso tiene el valor *MACJamming*. Dichas variables se incluyeron en el modelo de Función de Coordinación Distribuida (DCF, en inglés) implementado en el INETv3.4. Estos parámetros originalmente no forman parte del *framework*, fueron añadidos con el objetivo de alterar el funcionamiento del mecanismo DCF (*DcfUpperMac* en INET) en los nodos atacantes.

Durante la simulación los nodos atacantes intentarán bloquear las comunicaciones de los que se encuentren dentro de su rango de acción, escuchando en espera de una trama RTS y emitiendo una señal interferente en el momento en que algún nodo en su rango de alcance reciba una respuesta CTS. Los atacantes son externos a la red, es decir, no intervienen en el encaminamiento de paquetes ni utilizan la red para el intercambio de datos. Este comportamiento provocará una colisión de paquetes en las inmediaciones del nodo emisor de la trama RTS. El fenómeno es representado en la Fig. 2.

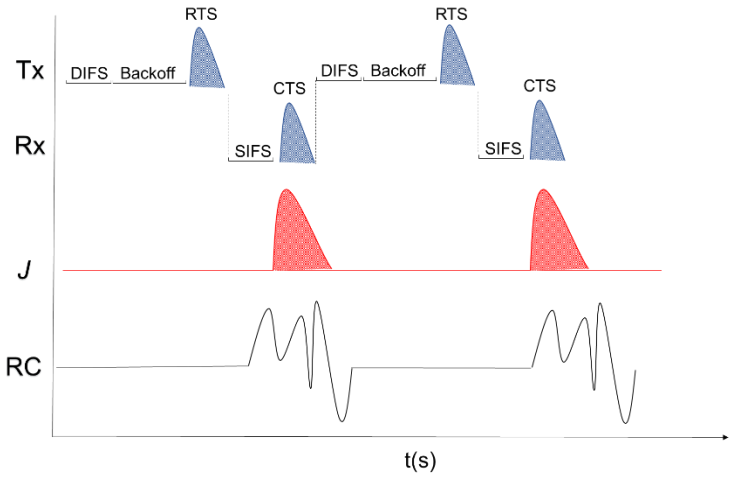

Figura 2: Ataque *MACJamming.* Tx: Transmisor, Rx: Receptor, *J: Jammer y* RC: Resultado de la colisión.

En este escenario se crearon 16 nodos del tipo *AODVrouter*, incluyendo dos nodos con funcionalidad de *gateway,* y dos nodos atacantes (*Jammer1* y *Jammer2*) ubicados estratégicamente (Fig. 3). El intercambio de paquetes se simuló utilizando aplicaciones que trabajan sobre el Protocolo de Datagrama de Usuario (UDP por sus siglas en inglés) como protocolo de transporte. Los módulos seleccionados para esta tarea fueron *UDPBasicApp* y *UDPSink*. La carga útil de los paquetes de aplicación se fijó a 512 Bytes y se transmitió a una razón de 1 paquete/segundo, y 1 paquete/0,8 segundos respectivamente, durante 100 segundos de simulación. Los puertos utilizados fueron 5000, 5001, 5002 y 5003. Los protagonistas de la comunicación, así como los tiempos de inicio y fin de la transferencia de paquetes, están descritos en la Tabla 1.

Tabla 1: Intercambio de tráfico. Ataque *MACJamming.*

Nodo fuente	**Nodo destino**	**Inicio (s)**	**Fin (s)**
N	K	0	100
L	Internet	5	100
Internet	L	5	100
M	N	10	100
*Jammer*1	-	0	100
*Jammer*2	-	50	100

Se utilizaron, además, dos tipos de tráficos: horizontal, entre los nodos de la capa de acceso (NCA), y vertical, entre estos e Internet, representada por un nodo también de tipo *AODVrouter*. Los rangos de transmisión en la capa de acceso se fijaron a valores de 50m (nodo K hasta nodo N) y 120m para el resto. De esta manera se pretendió simular una red de acceso en la que los usuarios tengan un alcance más limitado. Cada usuario que pretenda utilizar la red deberá hacerlo mediante los puntos de acceso (nodos H, I y J). En los primeros 50 segundos de simulación la red se encuentra solamente bajo el efecto del *Jammer 1* (Fig. 3A), sin embargo, a partir de los 50 segundos ocurre el ataque conjunto de los *Jammers* 1 y 2 (Fig. 3B).

TELEMÁTICA
REVISTA DIGITAL de las Tecnologías de la Información y las Telecomunicaciones
Revista Telemática. Vol.20 No.3 , Julio-Septiembre, 2021, p.49-60 ISSN 1729-3804

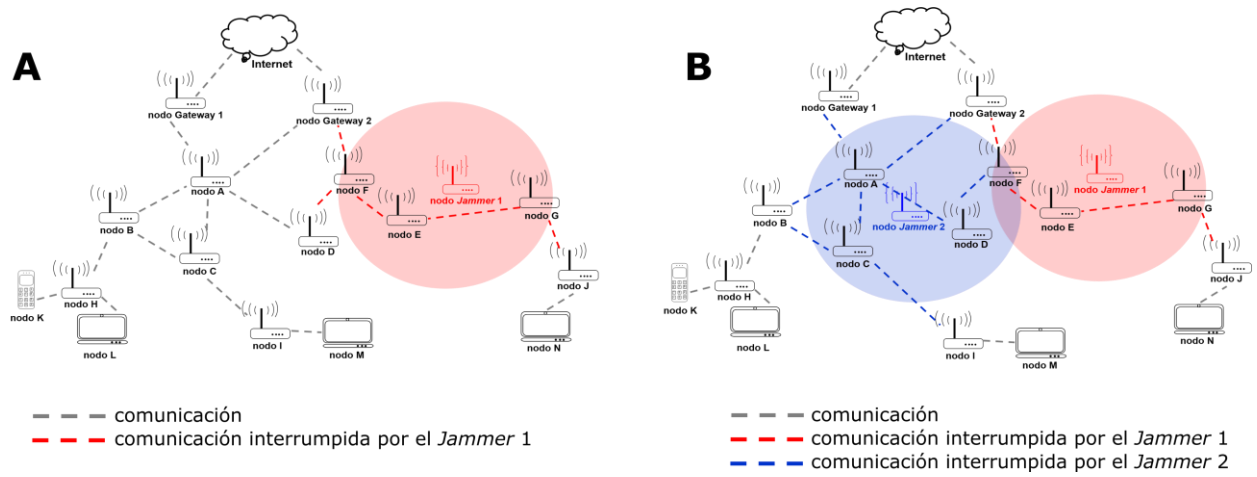

Figura 3: Topología infraestructura utilizada en el ataque *MACJamming*. **A**) Ataque realizado por el *jammer* 1 en un tiempo 0-50 s y **B**) Ataque conjunto de los *jammers* 1 y 2 entre los 50-100 s de simulación. Se resaltan con color rojo (jammer1) y azul (jammer 2) las áreas que cubre el ataque.

La Fig. 4 muestra los paquetes enviados por los nodos que intervienen en la comunicación. Por otra parte, la Fig. 5 muestra la recepción de paquetes en los nodos L, K, N y en el nodo Internet. La recepción exitosa hasta los 50 segundos se debe a que los nodos que intervienen en las rutas desde el nodo L hacia Internet (y viceversa), no se encuentran en el rango de alcance del nodo atacante *Jammer*1, por lo que la comunicación no se ve afectada. Sin embargo, el rango de transmisión de *Jammer*1 abarca la ruta por la cual se deben encaminar los paquetes desde N hasta K y desde M hacia N, es por ello que para estos nodos la recepción no es exitosa. Es decir, el total de paquetes recibidos es cero durante el tiempo de simulación. La Fig. 6 muestra la tabla de rutas para el nodo N a los 50 segundos de la simulación, en ella se puede apreciar que no contiene la dirección de ninguno de los nodos en la red. Posteriormente, a partir de los 50 segundos, comienza su operación el nodo atacante *Jammer*2, el cual interrumpe la comunicación entre los nodos L e Internet y es por ello que después de este tiempo la recepción de paquetes en toda la red es cero.

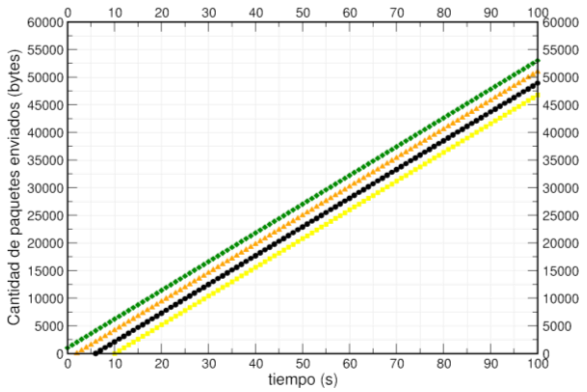

Figura 4: Paquetes enviados por los nodos N (verde), L (naranja), M (negro) y desde Internet (amarillo) comenzando en los tiempos establecidos.

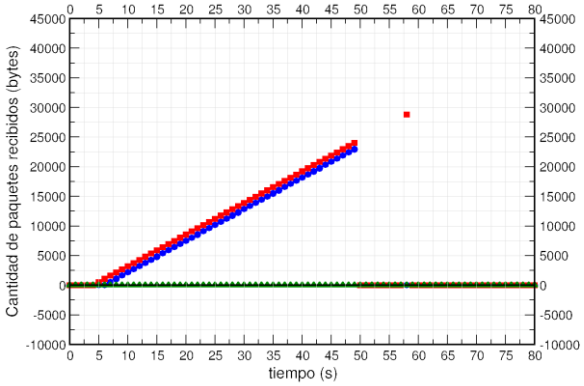

Figura 5: Paquetes recibidos por el nodo L (azul) y en Internet (rojo) y nodos con recepción interrumpida (verde).

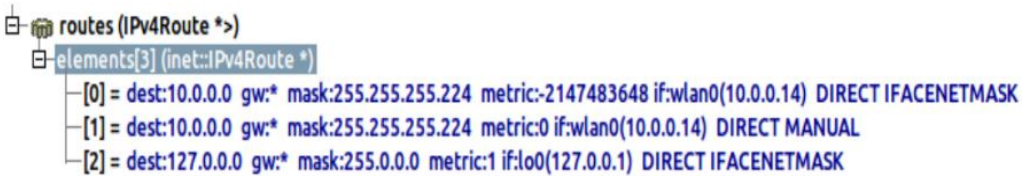

Figura 6. Tabla de enrutamiento del nodo N a los 50s de simulación.

Escenario 2. Ataque Flooding: El ataque *Flooding* en WMNs tiene el objetivo básico de consumir los recursos de la red en términos de batería y ancho de banda [15]. El nodo atacante ocupa el canal con la intención de utilizar todo el ancho de banda para transmitir sus tramas, impidiendo que el resto de los nodos intercambien paquetes en espera de la liberación del canal. En el Escenario 2 este comportamiento es simulado a través del envío de múltiples paquetes en un tiempo considerablemente pequeño y evitando el uso de tramas de control (RTS, CTS, ACK) en el nodo atacante. El resto de los nodos en la vecindad del nodo atacante obedecerán las reglas del protocolo IEEE802.11 y el intercambio de tramas RTS/CTS, por tanto, esperarán su turno para transmitir al detectar el medio ocupado. Para esta simulación no se considera la existencia de nodos atacantes externos. En cambio, se modifica el comportamiento de uno de los nodos que intervienen en el enrutamiento.

El nodo E fue seleccionado para comportarse de manera maliciosa a partir de un instante de tiempo. Este nodo comienza su operación de forma correcta y transcurridos 30 segundos inicia la inundación del canal con el envío de paquetes, incumpliendo las reglas del protocolo de control de acceso al medio (Fig. 7). Este comportamiento se mantendrá hasta los 40 segundos de simulación. La opción de utilizar el intercambio de tramas de control en el nodo atacante estará desactivada (parámetro *rtsThresholdBytes*), mientras que el resto de los nodos sí cumplirán con este requerimiento. Esto significa que el nodo malicioso no negociará su acceso al medio, simplemente enviará sus paquetes a una velocidad mayor al resto. Las especificaciones del medio inalámbrico son las mismas que se establecen en el apartado anterior. El intercambio de tráfico se establece entre los nodos y dentro del período de tiempo indicado en la Tabla 1. Los nodos seleccionados como destino son los que se encuentran en la vecindad del nodo E. De esta forma se pretende imitar la transmisión de paquetes en forma *broadcast.*

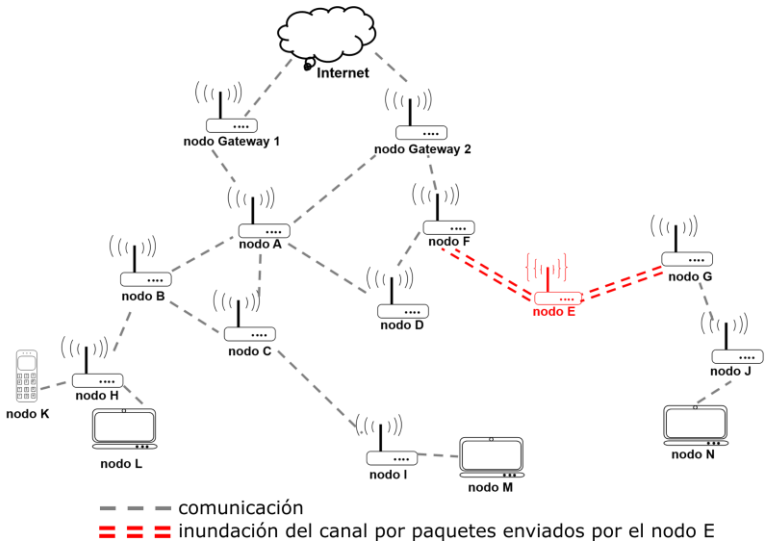

Figura 7. Topología infraestructura utilizada en el ataque *Flooding* de los 30-40 s de simulación.

El efecto de este ataque es similar al particionamiento de la red, pues las comunicaciones entre los nodos de la capa de acceso se interrumpen en el intervalo de operación del atacante como se muestra en la Fig. 8 (desde el segundo 30 al 40 de la simulación). Por otro lado, en la Fig. 9 se observa la fluctuación del valor de *throughput* en el intervalo de operación del nodo atacante.

TELEMÁTICA
REVISTA DIGITAL de las Tecnologías de la Información y las Telecomunicaciones
Revista Telemática. Vol.20 No.3 , Julio-Septiembre, 2021, p.49-60 ISSN 1729-3804

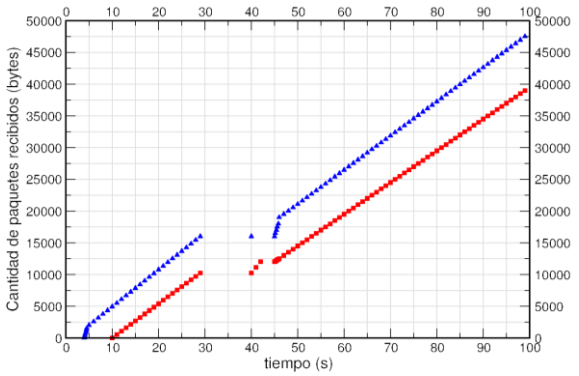

Figura 8: Paquetes recibidos por los nodos K (azul) y N (rojo).

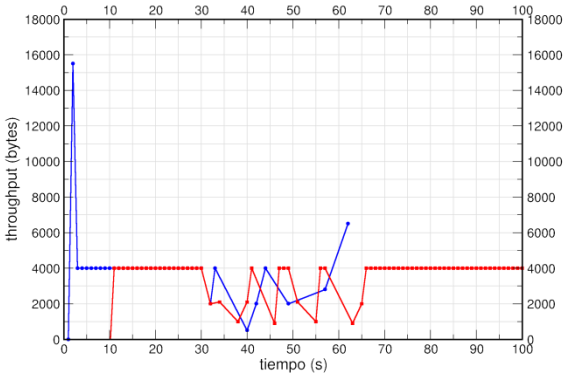

Figura 9: Variación del valor de *throughput* en los nodos K (azul) y N (rojo).

Discusión: Un atacante pudiera combinar los ataques antes descritos e interferir las tramas de control y al mismo tiempo, una vez ocupado el canal, transmitir sus datos. El mecanismo de *backoff* que ejecutan los nodos al no detectar una respuesta CTS luego de una solicitud RTS, modifica los tamaños de las ventanas de congestión, provocando que se transmitan paquetes cada vez más pequeños. Este comportamiento puede ser aprovechado por un nodo atacante para abarcar un mayor ancho de banda.

Sudhakar [16] realiza un estudio sobre una variedad de ataques de tipo *Jamming* selectivos, cuyas dianas son el canal de acceso, el enrutamiento, y el traspaso confiable de información *end-to-end*. En dicho trabajo se analiza la efectividad del *Jamming* selectivo sobre paquetes de datos y de control (SYN, ACK, DATA), cuya detección se hace aun más compleja. Posibles soluciones a este fenómeno incluyen la protección de los paquetes transmitidos mediante técnicas criptográficas. Como resulta evidente, este tipo de soluciones influyen fuertemente en la agilidad de procesamiento de cada paquete de información y, en consecuencia, reducen el rendimiento general de la red.

En [17] los autores analizan lo que ellos denominan "firmas" a nivel de paquete y a nivel de señal, expresadas por los nodos maliciosos durante el ataque. Estos parámetros pueden ser la elevada tasa de bit erróneo y la baja Relación Señal a Ruido, los cuales permiten la detección de dichos nodos y el aislamiento de la red como técnica de protección. La falta de mecanismos de defensa contra el ataque *flooding* deviene en una pérdida considerable de paquetes.

La ubicación del atacante en una posición estratégica respecto al resto de los nodos influye directamente en el impacto que tiene el ataque. En el caso de la topología usada en las simulaciones, existe un mayor número de variantes para alcanzar otros nodos, de ahí que los ataques no hayan sido completamente efectivos y algunos paquetes hayan alcanzado su destino. Esto demuestra que el grado de afectación de los ataques *flooding* y *MACJamming* depende en gran medida de la topología y la distribución (redundancia) de los nodos de las WMN.

Ataques al enrutamiento

A continuación, se aborda la simulación de dos ataques al enrutamiento, los cuales son muy comunes en las WMNs. Se describen escenarios que evidencian los efectos de los ataques *Sinkhole* y *Grayhole*, con el objetivo de determinar el grado de afectación que causan al comportamiento de estas redes. En las simulaciones se emplearon los protocolos AODV y OLSR (*Optimized Link State Routing* en inglés).

Escenario 3. Ataque Sinkhole: En este ataque el nodo malicioso selecciona y descarta intencionalmente algunos de los paquetes que le corresponde enrutar, o bien puede descartarlos todos. El nodo transmisor no cuenta con un mecanismo para detectar si el paquete ha sido entregado en el destino. Tampoco puede detectar si se está produciendo un ataque [18]. El nodo atacante envía información falsa de enrutamiento, proclamando que tiene una ruta óptima hacia el destino, provocando que otros nodos encaminen los paquetes de datos a través de él. La Fig. 10 muestra la posición y función de cada nodo de la red en ausencia del comportamiento malicioso del nodo 4 (Fig. 10A) y durante el despliegue del ataque (Fig. 10B). La Tabla 2 describe el intercambio de paquetes entre los nodos de la red, así como los tiempos de inicio y fin de cada intercambio. La tasa de envío en todos los casos es de 2 paquetes/segundo.

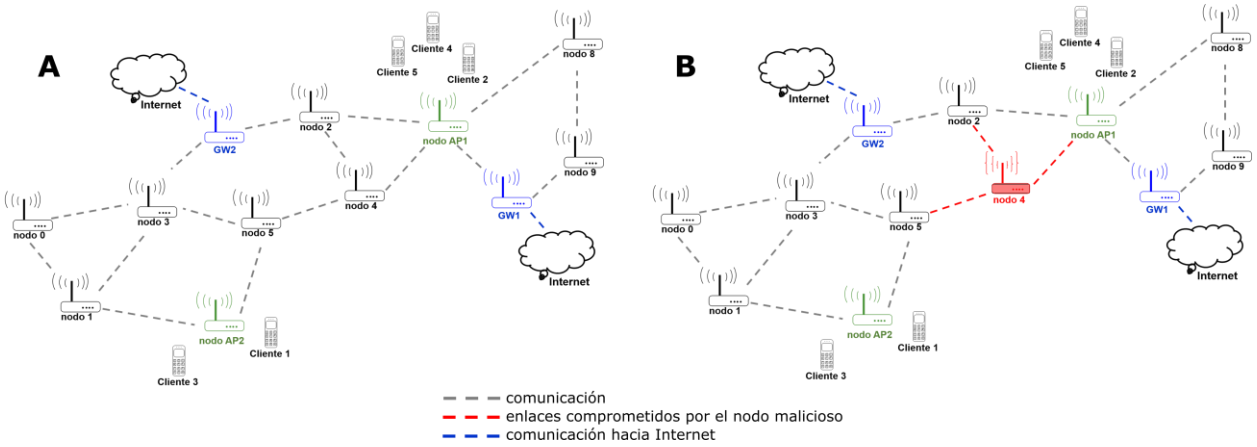

Figura 10: Escenario mallado diseñado para los ataques *Sinkhole* y *Grayhole.* A) Escenario entre los 0-15 s y 100-120 s de simulación. B) Ataque del nodo malicioso 4 (rojo) entre los 15-100 s de simulación.

Tabla 2: Intercambio de paquetes entre los nodos.

Nodo fuente	Nodo destino	Inicio (s)	Fin (s)
Cliente1	Internet	0	120
Cliente2	Internet	15	120
Cliente3	Internet	40	120
Cliente4	Internet	60	120
Internet	Cliente3	30	120
Atacante (Nodo4)	-	15	100

La Fig. 11 muestra los datos recogidos luego de la corrida en función de la cantidad de paquetes enviados y recibidos durante los 120 segundos de simulación. Inicialmente, el protocolo de enrutamiento utilizado es AODV. Puede apreciarse una considerable pérdida de paquetes en los nodos destinos a raíz del accionar del atacante, quien recibe la mayor parte de los paquetes para luego descartarlos. De un total de 870 paquetes enviados, solo 190 llegan a su destino (<22%), lo cual ocurre cuando el ataque se encuentra inactivo. En cambio, la Fig. 12 describe este mismo fenómeno, pero esta vez en función del tiempo. Una vez más se destaca el alto valor de paquetes siendo enrutados a través del nodo atacante (>78%).

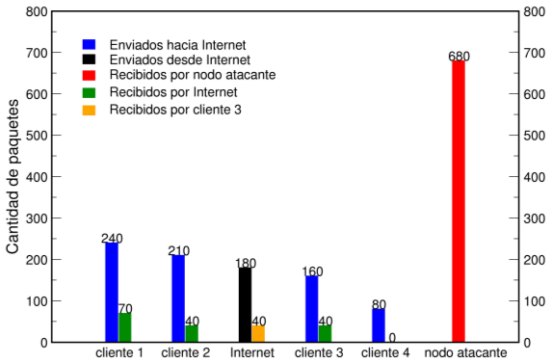

Figura 11: Intercambio de paquetes entre nodos de la red. Protocolo AODV.

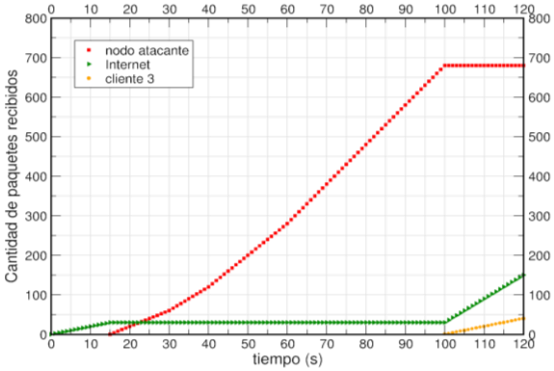

Figura 12: Paquetes recibidos en el tiempo de simulación. Protocolo AODV.

TELEMÁTICA
REVISTA DIGITAL de las Tecnologías de la Información y las Telecomunicaciones
Revista Telemática. Vol.20 No.3 , Julio-Septiembre, 2021, p.49-60 ISSN 1729-3804

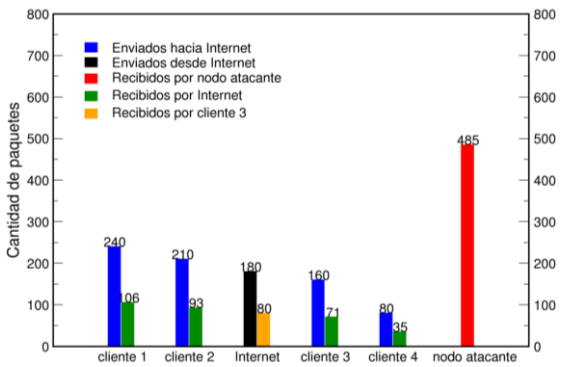

Figura 13: Intercambio de paquetes entre nodos de la red. Protocolo OLSR.

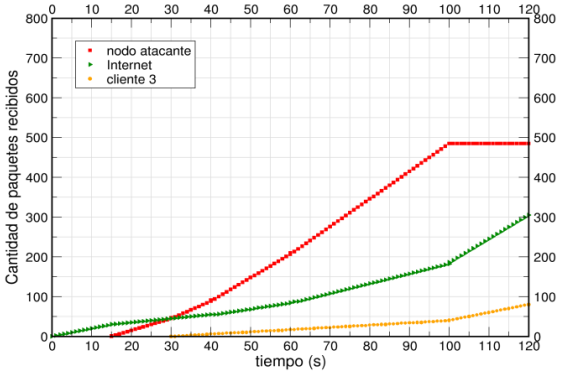

Figura 14: Paquetes recibidos en el tiempo de simulación. Protocolo OLSR.

Las Fig. 13 y Fig. 14 revelan una ligera mejora en el comportamiento de la red ante el ataque *Sinkhole* cuando se emplea el protocolo OLSR. En este caso es entregado en el destino el 44% de los paquetes, lo cual constituye una mayor tasa de entrega que para el caso anterior. Esto puede deberse al carácter proactivo del protocolo OLSR, el cual regularmente actualiza las tablas de rutas en cada nodo teniendo en cuenta la información generada y distribuida con los mensajes HELLO y de Control de Topología. Este comportamiento (aunque no combate este tipo de ataque o identifica el origen del mismo) permite elegir rutas alternativas de forma dinámica, minimizando el impacto del ataque. Por tanto, la designación de nodos MPR (*Multipoint Relay* en inglés) encargados de difundir dichos mensajes de control, resulta un paso clave en la configuración de la red mallada y afecta directamente su rendimiento [19].

Escenario 4. Ataque Grayhole: Para lograr un comportamiento que simule el ataque *grayhole*, se utilizó la combinación de dos ataques diferentes en el nodo atacante. Estos son los ataques *Sinkhole* y *Dropping* ya implementados en el *framework* NETA. Con el primero se garantiza que el nodo atacante envíe un mensaje de control falso en respuesta a un mensaje de solicitud de ruta generado por otro nodo. Con el segundo se fija el porcentaje de paquetes que van a ser descartados.

En el ataque *Dropping* los nodos descartan de forma intencionada, y con una cierta probabilidad, los paquetes de datos recibidos (en lugar de reenviarlos). La probabilidad de descarte puede ser configurada en el archivo .ini. De este modo se ve interrumpido el funcionamiento normal de la red. Según la aplicación afectada, el resultado puede ser una ralentización de la red debido a numerosas retransmisiones, un excesivo consumo de energía en los nodos, entre otros efectos. La Fig. 15 evidencia el comportamiento intermitente en la recepción de los paquetes, debido al carácter selectivo del ataque. El nodo atacante decide qué grupo de paquetes va a descartar. El valor de probabilidad de descarte puede ser modificado de forma tal que se dificulte aún más la detección de este nodo.

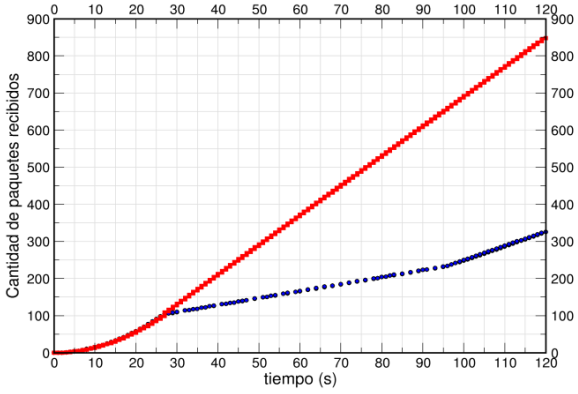

Figura 15: Paquetes siendo enrutados a través del nodo atacante (rojo) y paquetes recibidos por el nodo destino (azul).

Discusión: A partir de los resultados obtenidos en los escenarios descritos para los ataques *Sinkhole* y *Grayhole* resulta evidente que en todos los casos los ataques son efectivos. Estos afectaron de manera significativa la confiabilidad y robustez de las WMNs, por lo que se ratifica la necesidad de establecer mecanismos de seguridad que contrarresten el efecto de los mismos.

De forma similar a los casos anteriores, la ubicación del nodo atacante en una posición estratégica respecto al resto de los nodos de la red influye directamente en el impacto de los ataques. Adicionalmente, la selección de uno u otro de los protocolos de enrutamiento disponibles puede también ser determinante. En este caso, los protocolos proactivos presentan algunas ventajas que pueden ser aprovechadas para prevenir el efecto de los ataques DoS.

En el trabajo de Reddy y cols. [20] se realiza un estudio similar al presentado en este trabajo, pero limitado al efecto de ataques al enrutamiento en WMNs. En este caso NS (Network Simulator) es el escogido para la simulación de los escenarios con los ataques *Grayhole*, *Blackhole*, *Wormhole*, entre otros. Las mediciones sobre la tasa de paquetes recibidos y el *goodput* arrojan resultados similares a los presentados en esta investigación, teniendo en cuenta que también se emplea el protocolo AODV, para el cual resulta devastador el efecto de los ataques; entre los que se destaca el ataque *Wormhole* como el más severo.

Recientemente Babaeer y col. también utilizaron OMNET para simular el ataque *Sinkhole* [21], pero en escenarios de Redes de Sensores Inalámbricas. A diferencia del presente trabajo el impacto de los ataques es mitigado por la encriptación de paquetes y la autenticación de nodos, marcando a aquellos que expresan un comportamiento anómalo. La revisión bibliográfica demostró que un número importante de investigaciones utilizan el protocolo reactivo AODV en sus simulaciones debido a su factibilidad. Esto ocurre aun cuando el caso de estudio incluye ataques orientados a dañar el enrutamiento. Los resultados de este artículo, en cambio, demuestran que la elección de un protocolo proactivo como OLSR puede mitigar en alguna medida el daño del ataque. Si a esto se le añaden capacidades criptográficas o de detección de comportamiento o tráfico malicioso, cuidando mantener en un balance positivo la relación rendimiento y seguridad, entonces podrían alcanzarse soluciones factibles para ser empleadas en el entorno de las WMNs.

3. CONCLUSIONES

El despliegue de las WMN en Cuba puede ser una alternativa a los problemas existentes en el alcance de la conectividad, fundamentalmente en zonas rurales. Esta investigación puede constituir un punto de partida para investigaciones futuras, debido a que introduce herramientas como el OMNET, y el tema de simulación, en el contexto nacional. Fueron analizados cuatro tipos de ataques DoS, dos a la Capa de Enlace y dos a la Capa de Red de las WMN. En el caso de los primeros se demostró que las redes inalámbricas que utilizan el protocolo IEEE802.11, son susceptibles ante los ataques *MacJamming* y *Flooding*, y que no cuentan con mecanismos propios para combatirlos.

En el caso de los ataques *Sinkhole* y *Grayhole*, al enrutamiento de las WMN, los resultados evidenciaron que los protocolos proactivos como OLSR son más seguros que los reactivos, como AODV, frente a este tipo de ataques DoS, debido al método que utilizan para determinar las rutas. En el análisis de los resultados obtenidos también destacan otros aspectos que deben ser considerados en el momento de diseño y/o despliegue de las WMN, como es el caso de la redundancia de los nodos, el tipo de topología a utilizar, entre otros.

La elección de una técnica o grupo de técnicas como solución a un ataque específico o un grupo de ataques correlacionados, similares a los descritos en [20] debe, por tanto, tener en cuenta elementos sensibles en su operación. Algunos de estos elementos son: el consumo energético del nodo, el rendimiento general de la red (*delays*, *throughput*, *goodput*, *jitter*, tasa de pérdida de paquetes) y la integridad de la información que se transmite, entre otros.

REFERENCIAS

[1] M. A. Munawar, «Multi-Interface Multi-Channel Wireless Mesh Networks», Universidad de Waterloo, 2004.
[2] Y. F. Romero, «Algoritmo de distribución dinámica de canales basado en prioridades para Redes Malladas Inalámbricas multi-interfaces y multi-canales», Instituto Superior Politécnico José Antonio Echeverría, 2013.
[3] I. F. Akyildiz, «A Survey on Wireless Mesh Networks», *IEEE Radio Commun.*, vol. 47, no. 4, pp. 445 – 487, 2005.
[4] M. Molle, C., Voge, «A Quantitative Analysis of the Capacity of Wireless Mesh Networks», *IEEE Commun.*

Lett., vol. 14, no. 5, pp. 438–440, 2010.

[5] J. C.-M. Armuelles-Voinov y A. Chung-Cedeño, «Evaluation of QoS Provisioning in Nodes of Wireless Mesh Networks based on IEEE 802.11s», in *IEEE Central America And Panama Convention (Concapan XXXIV)*, 2014, pp. 1–5.

[6] A. K. Roy y A. K. Khan, «Performance Degradation in Wireless Mesh Networks via External and Internal Attacks», in *2019 2nd International Conference on Innovations in Electronics, Signal Processing and Communication (IESC)*, 2019, pp. 258–262.

[7] M. Abdelhakim, L. L. Jian Ren, y L. Tongtong, «Reliable Communications over Multihop Networks Under Routing Attacks», in *IEEE Global Communication Conference (GLOBECOM)*, p. 2015.

[8] R. Curtmola, J. Dong, y C. Nita-Rotaru, «Tradeoffs Between Security and Communication Performance in Wireless Mesh Networks», in *IEEE International Symposium on "A World of Wireless, Mobile and Multimedia Networks" (WoWMoM)*, 2010, pp. 1–6.

[9] H. Silva, M. Nogueira, y A. Santos, «A Cross-layer and Adaptive Scheme for Balancing Performance and Security on WMN Data Routing», in *IEEE Global Telecommunications Conference (GLOBECOM)*, 2010, pp. 1–5.

[10] K. Sundaramoorthy y S. S. Rao Madhane, «The Effect of Secure Routing with QoS Amplification (SRQA) in Wireless Mesh Networks», in *Second International Conference on Current Trends In Engineering and Technology (ICCTET)*, 2014, pp. 484–488.

[11] «IEEE Standard for Information technology–Telecommunications and information exchange between systems local and metropolitan area networks–Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications», pp. 1–3534, 2016. doi: 10.1109/IEEESTD.2016.7786995

[12] I. F. Akyildiz y X. Wang, *Wireless Mesh Networks*. 2009 pp. 2-4.

[13] X. Wei, Q. Wang, T. Wang, y J. Fan, «Jammer Localization in Multi-Hop Wireless Network : A Comprehensive Survey», *IEEE Commun. Surv. Tutorials*, vol. 19, no. 2, pp. 765–799, 2016.

[14] J. Peng y L. Cheng, «Revisiting Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)», in *2006 40th Annual Conference on Information Sciences and Systems, Princeton*, 2006, pp. 1236–1241.

[15] A. Sana, F. Youssef, y R. M. Driss, «Flooding Attack on AODV in WSN», in *Renewable Energies, Power Systems & Green Inclusive Economy (REPS-GIE)*, 2018, pp. 1–5.

[16] M. Sudhakar, «A Study Of Wireless Mesh Networks Insider Attacks Of Selective Jamming Or Dropping», *IOSR J. Electron. Commun. Eng.*, vol 11, no. 2, pp 60-66, 2016

[17] A. Ansari y M. A. Waheed, «Flooding Attack Detection and Prevention in MANET Based on Cross layer Link Quality Assessment», in *International Conference on Intelligent Computing and Control Systems ICICCS*, 2017, pp. 612–617.

[18] B. Venkataramana y A. Jadhav, «Performance Evaluation of Routing Protocols under Blackhole Attack in Cognitive Radio Mesh Network», in *International Conference on Emerging Smart Computing and Informatics (ESCI)*, 2020, pp. 98–102.

[19] Y. Mostafaei y S. Pashazadeh, «An Improved OLSR Routing Protocol for Reducing Packet Loss Ratio in Ad-hoc Networks», in *Eighth International Conference on Information and Knowledge Technology (IKT)*, 2016, pp. 12–17.

[20] K. G. Reddy, M. S. Sudheer, P. K. Sree, V. P. Raju, «Simulation analysis on network layer attacks in wireless mesh networks», *Int. J. Eng. Technol.*, vol 7, no. 3.29, pp 301-303, 2018.

[21] H. A. Babaeer y S, A. Al-Ahmadi, « Efficient and Secure Data Transmission and Sinkhole Detection in a Multi-Clustering Wireless Sensor Network Based on Homomorphic Encryption and Watermarking», *IEEE Access,* vol 8, pp 92098-92109, 2020.

SOBRE LOS AUTORES

Damian Ruiz-Varona, ORCID 0000-0003-0727-1500. Ingeniero en Telecomunicaciones y Electrónica (2017). Desarrolla su actividad investigativa en el estudio de las Redes Malladas Inalámbricas.

Anays Guilarte-Acosta, ORCID 0000-0002-2052-3621. Ingeniera en Telecomunicaciones y Electrónica (2017). Desarrolla su actividad investigativa en el estudio de las Redes Malladas Inalámbricas.

Walter Baluja García, ORCID 0000-0003-3499-4843]. Rector de la Universidad de Ciencias Informáticas. Doctor en Ciencias Técnicas (2007). Desarrolla su actividad docente-investigativa en los temas de Informatización y, de

Arquitectura, Gestión y Seguridad de Redes. Ha presentado más de 50 ponencias y conferencias en eventos internacionales y, tiene más de 30 artículos publicados.

CONFLICTO DE INTERESES

No existe ningún conflicto de intereses de los autores o de las instituciones a las cuales pertenecen en relación al contenido del artículo aquí reflejado.

CONTRIBUCIONES DE LOS AUTORES

- **Damian Ruiz-Varona**: conceptualización, preparación, creación, organización y desarrollo del artículo.
- **Anays Guilarte-Acosta**: conceptualización, preparación y sugerencias acertadas para la conformación de la versión final.
- **Walter Baluja García**: contribución a la idea, revisión crítica de cada una de las versiones del borrador del artículo y aprobación de la versión final a publicar.