International Journal of Computer Information Systems and Industrial Management Applications.
ISSN 2150-7988 Volume 13 (2021) pp. 252-265

Received: 7 January 2021; Accepted: 21 May 2021; Published: 15 August 2021

Avoiding Wormhole Attack in MANET Using an Extending Network Knowledge

Hicham Zougagh[1], Noureddine Idboufker[2], Rachid Elayachi [1] , Youssef Saadi [1], Samir Elouaham[3] and Azzdine Dliou[4]

[1] Faculty of Sciences and Techniques, Moulay Slimane University,
Beni Mellal, Morocco
h.zougagh@usms.ma

[2] National School of Applied Sciences, Cady Ayyad University,
Marrakech, Morocco
n_idboufker@yahoo.fr

[3] Faculty of sciences, Chouaib Doukkali University,
El jadida, Morocco
elouahamsamir@gmail.com

[4] Faculty faculty of applied sciences, Ibn Zohr University,
Agadir, Morocco
dliou.azzedine@yahoo.fr

Abstract: **The shared nature of the Ad hoc networks makes it essential to secure them in order to guarantee a better reliability of the application services using their infrastructure. Indeed, the specific characteristics of ad hoc networks, such as the absence of infrastructure, the absence of a central trust unit, and the use of the radio channel, require the development of specific solutions to secure these networks, taking into account the constraints related to the cooperation between nodes, mobility, energy and free access to the medium. The work done in this paper focuses on the contribution to the improvement of network security through the strengthening of security in the case of multi-hop wireless networks and more particularly the detection of malicious nodes that can affect the control plane of the network layer. We have contributed to the development of new solutions to deal with the black hole attack in the case of the OLSR protocol widely used in the ad hoc context. Black hole is an attack that can be carried out by one malicious node or a coalition of several malicious nodes. The Optimized Link State Routing Protocol is developed for Mobile Ad Hoc Networks. It operates as a Table driven, proactive protocol. The core of the OLSR is the selection of Multipoint Relays (MPRs), used as a component of a flooding mechanism. MPRs distribute control traffic messages within the network while reducing the redundancy in the flooding process. An OLSR node selects its MPR set in a manner that all two hop neighbors are reachable by the minimum number of MPRs. However, if an MPR misbehaves during the control phase, the network connectivity is then compromised.**

This paper introduces a new Multipoint Relays (MPR) selection algorithm with additional coverage. It also specifies an extension of the OLSR protocol in order to provide multiple disjoint paths especially for dynamic topologies. Disjoint paths are helpful for increasing network throughput, improving forwarding reliability, load balancing and security.

Keywords: MANET, OLSR protocol, Security, Attack, Wormhole, Intrusion.

I. Introduction

An ad hoc network consists of wireless devices that can communicate without a fixed infrastructure. In a mobile ad hoc network (MANET), the network topology can change dynamically since nodes can move in an unpredictable way. Nodes are free to move at any speed, to in any direction and to join or to leave the network at any time. MANET, is formally defined as an autonomous system of nodes. This network can be modeled as an arbitrary communication graph. In multi-hop network, nodes can also act as intermediate hop or router belonging to a path connecting a source and a destination nodes. Paths are formed using one of several standard or customized routing protocols.

Several protocols exist, addressing the problems of routing in MANET. Such protocols are, traditionally, divided into two classes, depending on when a node acquires the knowledge about the route to a destination. Reactive protocols such as AODV (Ad hoc On demand Distance Vector Routing) [1] and DSR (Dynamic Source Routing) [2] are characterized by nodes acquiring and maintaining routes on-demand. In this case, when a route to a new destination is required, a query is flooded onto the network and replies containing possible routes to the destination are returned. In the proactive approach, every node exchanges routing informations in order to maintain and construct routing tables even if there is no data traffic to deliver. Information contained in routing tables, is updated when the topology changes. In the case of OLSR (Optimized Link State Routing) [3] and DSDV (Destination Sequenced Distance Vector Routing)[4], every node

maintains updated routing informations to every other node in the network.

Ad hoc mobile networks are confronted with numerous problems due to their intrinsic characteristics, making the security solutions developed for wired networks or networks with infrastructure, generally, not adapted to the context of Ad hoc mobile networks. Indeed, security in ad hoc networks is a rather complex problem due to the conjunction of several factors that increase the vulnerability to various types of attacks that can be launched in a relatively simple way. Indeed, the use of wireless connections facilitates eavesdropping, allowing the analysis of network traffic and making it possible to launch active attacks.

Identity spoofing is another type of attack that is easily accomplished in the wireless environment. Indeed, with physical access to the network, any machine is able to reach out to other machines on the network, create attacks and disrupt network activity without being detected. Furthermore, an attacker who is familiar with the mechanisms of the physical and MAC layer and who has sufficient transmission power can prevent his neighbors from accessing the communication channel. Because of all these vulnerabilities that characterize wireless communication, malicious nodes can modify, spoof, inject data, generate false messages, and generally not respect the protocols used. The impact of such malicious behavior can be severe, especially since the cooperation of nodes throughout the network acts as the infrastructure.

Since the operation of ad hoc networks relies entirely on cooperation between its entities, significant degradation can be expected when entities attempt to abuse the basic operations that are in their charge. Unfortunately, most ad hoc routing protocols do not incorporate security control mechanisms, as they assume truthful behavior among the collaborating entities. However, the reality can be very different in the presence of malicious entities capable of performing intrusions by exploiting vulnerabilities in the ad hoc infrastructure. Attacks on routing in MANETs, whether motivated by selfishness or maliciousness, include the dissemination of erroneous routing information, and the suppression or non-retransmission of routing or data traffic, this attack is known as a black hole. Such behavior disrupts the overall operation of the network, as it can cause the formation of longer paths, and loss of connectivity between entities.

The subject of this paper is the study of the problem of security of ad hoc networks, and more precisely the security of the routing process, with the objective of ensuring the integrity and confidentiality of information without forgetting the continuity of service within an ad hoc network.

While attacks against routing operations are easy to implement, they are particularly difficult to contain. Numerous proposals have been made to ensure the security of routing protocols against the suppression of information either at the signaling level or at the data routing level. These solutions can be classified into three categories:

Cryptography-based solutions: Several security architectures have been proposed to distribute encryption keys and certificates in order to secure communication between nodes. However, most of these architectures do not respect the characteristics of MANETs.

Reputation-based solutions: these consist of a monitoring mechanism to identify entities causing malicious behavior, a reputation calculation mechanism, and a response mechanism. These systems are typically used to detect selfish entities and force them to cooperate. Nevertheless, a dishonest entity can have a good reputation because it participates in network operations, while behaving badly because it spreads false information.

Solutions based on trust management systems: that use the intrinsic properties of routing protocols to search for inconsistencies between exchanged messages. These solutions operate as an intrusion detection system against internal attacks. On the other hand, these solutions do not completely deal with situations in which a malicious entity attempts to abuse the security mechanisms, either individually or more subtly through a coalition with other entities.

Routing process is fundamental for MANETs. Thus, it constitutes a privileged target of attackers. In fact, malicious nodes can compromise the routing protocol functionality by disturbing the route discovery process and consequently corrupting network functioning and degrading its performances.

OLSR [3] is a proactive routing protocol for MANET, i.e. All nodes need to maintain a consistent view of the network topology. They are also vulnerable to a number of disruptive attacks in the presence of malicious nodes (identity spoofing, link withholding, link spoofing, miserly attack, wormhole attack and Black hole attack...). As a result, it is primary to implement and improve security schemes for the OLSR protocol.

In this paper, we investigate a specific type of attacks, known as wormhole attack. Such attacks Are launched between two malicious nodes. These malicious nodes are distant from each other and each of them sends the received packets to the second peer node through a wormhole tunnel. Then the peer node resends the packets to the original destination. In this way, two malicious nodes seem to be one-hop neighbors and the path used between these two nodes looks shorter than the actual path between the source and the destination [5]. Therefore, the malicious nodes deceive the normal nodes and disturb the routing process [6].

The rest of the paper is organized as follows. The next section provides a short overview on OLSR, followed by the description of wormhole attack. Section 4 summarizes the literature. In section 5, we present our new approach aiming to secure OLSR protocol while Section 6 presents simulations results. In the end Section 7 concludes the paper.

II. Optimized Link State Routing Protocol

OLSR (Optimized Link State Routing Protocol) [7] is a proactive routing protocol that uses periodic exchanges of HELLO messages to allow each node to know its one-hop and tow-hop neighbors. It is the result of an optimization of the link-state protocol of wireline networks. Its innovation consists in its ability to save radio resources when broadcasting control traffic by using the concept of Multipoint Relays so that a subset of links connecting a node with its neighbors are declared instead of all the links, these links are the ones that connect it to its MPRs.

The OLSRv2 protocol has the same algorithm and the same mechanism concerning the flooding of Multipoint Relays. Being of modular architecture it is composed of a number of blocks, independently standardized and applicable in other

protocols: RFC 5148 takes into account the jitter in MANETs [8], RFC 5444 is a generalization of packet and message formats [9] and RFC 5497, represents a multitude of temporal values in Ad Hoc networks [10]. NHDP [11] is a neighbor discovery protocol also used by OLSRv2.

A. Discovering Neighbors

Ad hoc networks are characterized by a changing topology. To detect any changes in the network and generate topology information. OLSR nodes exchange HELLO and TC messages. These messages are used to determine the best path to reach each destination.

During the neighborhood detection, each node regularly transmits HELLO messages to signal its presence and its links with its neighbors, which allows the nodes to build and maintain several sets: Link set (LS: includes all neighbors), Neighbor set (1HN_set: includes only symmetric neighbors), two hop Neighbors set (2HN_set: includes the symmetric neighbors of its neighbors) and the MPR neighbors set (MPR_set). Each node stores the addresses of those neighbors that have selected it as MPR in the MPRSS_set.

From this information, each node maintains in a set called Topology set (T_set) the information about the destination points in the network. A node that has been selected as MPR periodically sends TC messages announcing the list of its symmetric neighbors that have selected it as MPR. This TC message is only retransmitted by the nodes that it has chosen as MPR.

B. Multi-Point Relays Selection

Each node builds its set of MPRs to create a subset of one-hop neighbors with symmetric links that covers all two-hop neighbors. A node's MPRs are declared in subsequent HELLO messages transmitted by that node so that the information can reach the MPRs themselves.

The MPR_set of a node is the union of the MPR_set relative to each interface. Moreover, in each HELLO message, nodes include a WILLINGNESS field that specifies the ability of a node to participate in the packet retransmission mechanism. At a given time the node must declare the same value in the WILLINGNESS field for all its interfaces. Its values are all as follows:

WILL_NEVER: This node should not be selected as MPR.
WILL_ALWAYS: This node should always be selected as MPR by all its neighbors.
WILL_DEFAULT: This is the default value.

C. Declaration of Multi-Point Relays

Each node selected as MPR periodically broadcasts TC (topology control) messages to all nodes in the network, to build up an information base related to the network topology (Topology_set). The TC messages are transmitted by the nodes in the network at regular time intervals and with a Time To Live (TTL=255) so that each MPR can declare the list of neighbors that have selected it as MPR in the whole ad hoc network. The list of addresses of the MPR selectors of an MPR node can be split and broadcast over several TC messages (this is due to the limitations on the volume of the TC message imposed by the protocol). A node only retransmits the TC message if it is sent by a node contained in its selector MPR set.

The topology table is updated each time a TC message is received:

T_des_addr : it is the identifier of a destination node (MPR selector contained in TC).
T_last_addr : it is the identifier of the last node that allows to reach the destination.
T_seq : a code generated by the source relative to these MPR selectors.
T_time : the duration of time after which the information contained in this tuple is expired.

D. Routing Table Calculation

Each node maintains a routing table that allows it to route packets to known destinations. These routing tables are computed based on information about the network topology and link status with its neighbors. A DijKstra shortest path algorithm [12] is used to compute the optimal route between the local node and the destination node. In addition, OLSR allows nodes to recompute their routing tables whenever there is a change in the different sets maintained by each node, namely: Link set, 1HN_set, 2HN_set, Topology_set. Each routing table entry is composed of:

R_dest_addr: identifies the address of the destination node.
R_next_addr: contains the address of the next node (one hop away) to reach the destination.
R_dist: the number of hops between the local node and the destination.
R_iface_addr: the interface through which to reach the destination.

These entries specify that the node R_dest_addr is estimated to be R_dist hops away from the local node and that the first hop to reach the destination through the interface R_iface_addr is R_next_addr.

E. Packet and message format in OLSR

OLSR allows nodes to communicate using a single packet format model for the transmission of all protocol-related data. This facilitates protocol extension without breaking up compatibility and also allows different messages to be sent in a single packet structure.

Each packet encapsulates one or more messages. The messages share a common header format, which helps nodes to transmit messages correctly.

According to the objective of each operation, OLSR allows the diffusion of the messages in all the network to share the topology of the network or simply a limited diffusion for the discovery and the declaration of the neighbors.

1) Format of the header of messages and Packets in OLSR.

The basic scheme of OLSR packets is given in Figure 1 (neglecting IP and UDP headers).

Packet Length: This field represents the length of the packet in bytes. If this length is less than or equal to the size of the packet header, the message is ingested.

Packet Sequence Number (PSN): The PSN is incremented by one each time a new OLSR packet is transmitted. The PSN is used to discard packets already processed and stored in the Duplicate_set table.

Message Type: This field indicates the type of message included in the packet (Hello, TC,...). Several message types can be transmitted in the same packet.
Vtime: This field shows how long after a message is received a node considers the information contained in the message to be valid unless a more recent update of the information is received.
Message Size: This field indicates the size of the message, counted in bytes and measured from the "Message Type" field to the beginning of the next "Message Type" field, or to the end of the packet if there is no next message.
Originator Address: Contains the primary address of the node generating the message. This field should not be modified in the message retransmission mechanism.
Time to Live: This field contains the maximum number of hops that a message can reach. Before the retransmission of each message the TTL field must be decremented by one. In case the TTL value of a message is equal to 0 or 1 this message should not be retransmitted.
Hop Count: This field contains the number of hops a message has reached. Before a message is retransmitted, this field must be incremented by one. At the beginning the generator sets the Hop Count to zero.
Mesage Sequence Number: During the message generation procedure the source will assign to each message an identifying number, this number is called Message Sequence Number. The Sequence Number is incremented by one for each message generated by the node. Sequence numbers are used to ensure that a given message is not retransmitted more than once.

Packet Leng		Packet Sequence Number
Message Type	Vtime	Message Size
Originator Address		
Time To Live	Hop Count	Message Sequence Number
MESSAGE		
Message Type	Vtime	Message Size
Originator Address		
Time To Live	Hop Count	Message Sequence Number
MESSAGE		

Figure 1. General format of an OLSR package

2) HELLO Message Format

Hello messages are broadcast periodically by a node to signal its presence and its links with its neighbors (these messages will not be retransmitted). The exchange of Hello messages allows a node to detect different types of neighbors and to signal Multipoint Relays. For this purpose and taking into consideration future extensions of the protocol, an approach similar to the global packet format is taken into account, therefore the proposed format of a Hello message is schematized in Figure 2 according to the OLSR specifications [13]:

Reserved: this field must be set to the value " 0".
Htime: This field specifies the frequency of the transmission of Hello messages on each interface of the node.
Willingness: This field reflects the ability of a node to relay a message to another node. A node with a Willingness equal to WILL_NEVER should never be chosen as MPR by other nodes. On the other hand, nodes with a Willingness equal to will_ALWAYS must always be chosen as MPR. In the normal case of the protocol a node would have to announce a default Willingness equal to WILL_DEFAUT.
Link Mssage Size: measures the size of the link message, counted in bytes and measured from the "Link Code" field to the next "Link Code".
Neighbor Interface Address: the address of a neighbor's interface.

Reserved		Htime	Willingness
Link Code	Reserved	Link Message Size	
Neighbor Interface Adress			
Neighbor Interface Adress			
……			
Link Code	Reserved	Link Message Size	
Neighbor Interface Adress			
Neighbor Interface Adress			
……			

Figure.2 : General format of an OLSR message

The Link code field has a size of 8 bits, but the OLSR specification only uses the first 4 bits. This part contains both the information about the links to the neighboring nodes and the type of the latter. Tables. 1 and Figure.3 illustrate the different possible values for the two fields Neighbors type and Link Type.

0	1	2	3	4	5	6	7
				NeighbrType		**Link Type**	

Table 1 : Link code

Link Type	
UNSPEC_LINK	No information on the type of link is given
ASYM_LINK	Indicates that the interface is detected.
SYM_LINK	Indicates that the link with the interface is symmetrical

	and can be considered as a neighbor
LOST_LINK	the link is lost
Neihgbor Type	
SYM_NEIGH	Indicates that the neighboring node has at least one symmetric link to the local node.
MPR_NIGH	Indicates that the neighboring node has at least one symmetric link to the local node and has been selected as an MPR by this node.
NOT_NEIGH	This type of neighbor indicates that the node cannot be considered a neighbor or that it has not yet become a symmetric neighbor.

Figure 3. The possible values for the Link Code field

3) Topology Control Message Format

In order to build the routes for all the destinations, each node of the ad hoc network announces the nodes they have chosen as MPRs (i.e. the MPR selectors) through TC messages. These are sent as given in the message part of the packet with a "Message Type" equal to TC_MESSAGE, and the Time To Live field must be equal to 255 so that the information can reach the whole network.

The format proposed by [14] is shown in Figure.4

ANSN	Reserved
Advertised Neighbor Main Address	
Advertised Neighbor Main Address	
……	

Figure 4. Format du message TC

Reserved: this field must be set to "0".
Advertised Neighbor Sequence Number (ANSN): A sequence number is associated with the set of neighbors of the sending node. Each time a node detects a change in the set of neighbors, it increments this sequence number. This sequence number is sent in this ANSN field of the TC message to keep track of the most recent information. When a node receives a TC message, it can decide, based on this sequence number, if the information received about the generator node's neighbors is more recent than the one already received.
Advertised Neighbor Main Address: This field contains the main address of the neighboring node. All main addresses of the generator node's neighbors are put in the TC message.

III. Wormhole attacks in OLSR

In a typical wormhole attack, the attacker receives packets at one point in the network and forwards them through a wireless or wired link with much less latency than the default links used by the network. Furthermore, it then relays them to another location in the network [7]. Since a wormhole attack can affect the topology construction mechanism especially in the case of proactive routing protocols such as OLSR due to the periodic exchange of control packets for neighbor discovery and topology construction.

-

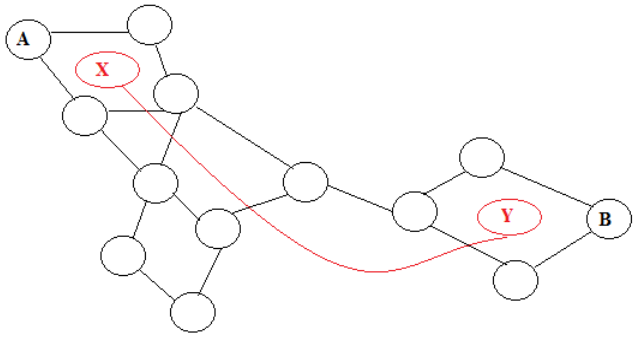

Figure 5. Wormhole tunnel constructed between nodes X and Y

When node A broadcasts its HELLO message, node X (attacker 1) copies this HELLO message and tunnels it to node Y (attacker 2) through the constructed wormhole. Y receives A's HELLO message and replays it to its neighbors. When node B receives the replayed HELLO message, B deems node A to be its one-hop neighbor. Following a similar procedure, node A may be brought to assume node B to be its one-hop neighbor. After a certain time, a symmetric link can be established between A and B according to the OLSR mechanism. Once this spoofed symmetric link is established, A and B are very likely to choose each other as MPRs. This situation leads to an exchange of some TC messages and data packets through the wormhole tunnel (Figure 2).

Out of all the attacks on a Ad Hoc Network, wormhole attack is a brutal one as it exploits confidentiality, availability, and overall security of the MANET. The drastic impact on the network due to the instigation of the wormhole attack is discussed below:
Manipulation of routing protocols: The wormhole attack significantly deteriorates the functioning of network protocols by taking control over the routing traffic of the sensor network. Once an intruder gets access to routing information, it effects neighborhood discovery by creating fake list of neighbors and disrupts network functioning by dropping data packets [15] [16].
Layout for several other attacks: The wormhole attack serves as a l-ayout for several other harmful attacks which are mentioned below:

i. Rushing attack: An attacker in a wormhole attack is able to attract traffic from the neighboring nodes if the wormhole link being established has a faster transmission rate. This in turn results in rushing attack where all the packets in the network adapt this fast wormhole link as their transmission channel, leading to an increase in the average attack success rate [17].

ii. Sinkhole attack: While performing the wormhole attack, the malicious nodes present at the two ends of the tunnel gathers required information so as to launch sinkhole attack in the sensor network [15].

iii. Selective forwarding attack: Wormhole attack can also further lead to selective forwarding attack as an intruder can block and drop certain packets through the two malicious nodes that form the wormhole tunnel [15].

IV. Classification of Wormhole Attack

A. Based on the absence or presence malicious node.

The malicious nodes and their packet forwarding behavior during tunneling and replaying of packets, the wormhole attack occurs in two different modes, namely hidden and exposed modes, respectively [18].

Hidden Mode: In this mode, the malicious nodes present in the network do not manipulate the content of the data packets and the AODV packet header while transferring the packets from one end of the tunnel to the other end.

Exposed Mode: The attacker manipulates the contents of data packets in exposed mode by including its identity while transferring packets in the tunnel. However, the malicious nodes do not mess with the AODV packet header, and it remains unaltered [16].

B. Based upon the implementation method used

the wormhole attack can be classified into the following categories:

1) Out-of-band channel: In this mode, the malicious nodes are connected by a high quality and high bandwidth out-of-band channel in order to launch the wormhole attack. The tunnel thus established can be constructed either by using a wired link or a directional wireless link. This mode requires specialized hardware for implementation making it more difficult to launch compared to other methods such as encapsulation [19, 20].

2) Packet Encapsulation: Implementation of wormhole attack becomes easy with the use of encapsulation method as it does not require any special hardware, plus the ends of the wormhole link do not contain any cryptographic data. In this mode, the two malicious nodes contain several sensor nodes in between and the data packets flowing between them are encapsulated. Due to this encapsulation, the actual hop count of the nodes does not get incremented and the data packets are transformed to their original form at the end point of the tunnel [18][20].

3) Packet Relay: Wormhole attack can be launched by packet relay method using one or more malicious nodes. In order to create fake list of neighbors, the attacker convinces two remote sensor nodes that they are neighbors by replaying packets between them [20].

4) High Power Transmission: This type of wormhole attack is launched by a single malicious node with a high power transmission capability. The malicious node transfers data packets to other sensor nodes from a remote distance at high power so as to establish itself into the path between the source and destination [20].

C. Based upon the medium used to implement the wormhole attack.

it is classified into the following two types:

In-band: In in-band wormhole attack, the same existing medium is used to establish the tunnel between two malicious nodes. In-band medium is the most common choice and is used by encapsulation, packet relay, and protocol deviation methods to launch the wormhole attack [19][21].

Out-of-band: An attacker in the out-of-band method does not use the same medium but different wireless network to achieve wormhole attack [21].

D. On the basis of the behavior of the sensor nodes.

while forwarding packets, visibility of intruders, and the identities of the wormhole nodes, the wormhole attack is categorized into three types: open, half-open, and closed wormhole attack.

1) Open wormhole: The source and destination nodes as well as the two ends of the wormhole link are visible in open wormhole attack. The identities of the attackers are visible in the header of the data packets involved in route discovery. The sensor nodes think of the malicious nodes as direct neighbors although they are aware of the presence of these bogus nodes along the route.

2) Half-open wormhole: One end of the wormhole link is visible, while the other is kept hidden. The contents of the data packets are not altered but are simply forwarded from end of the tunnel to the other end.

3) Closed wormhole: The attacker in this mode creates a fake list of neighbors by creating an illusion that the distance between the source and the destination is of one hop. Also, the visibility of the source node, destination node, and two end nodes of the tunnel are not disclosed [18].

V. Related Works

Several approaches have been developed to manage wormhole attacks in mobile ad hoc networks.

Hu et al. [8] presented the geographic packet leash. Making use of appending location information about sending nodes in every packet, they check whether hop-by-hop transmission in the network is physically possible or not and consequently detect the presence of wormholes. Wang et al. [22] in their work verified the end-to-end distance limits between the source node and the destination node. Zhang et al. [23] in their work proposed a neighborhood scheme based on location for authentication in order to find the wormholes. These approaches make use of the pre knowledge of the node locations so as to find the difference in the distance.

Khalil et al. [24] proposed the scheme LiteWorp; it assumes the presence of attack-free situation before the launch of wormhole attack. During the deployment phase, each network node gathers its two hop neighbors and LiteWorp followed by selecting the guard nodes for wormhole channels detection. This is done by overhearing transmissions that are infeasible among the non neighboring nodes. They also proposed a

complement to LiteWorp called MobiWorp [25], making use of the assistance of some location aware mobile node.

Song et al. [25] in their work monitor the truth that wormhole links are chosen for high-frequency routing, and, by matching this with regular statistics, wormhole links can be identified.

Singh et al. [27] have proposed a cross-layer based intrusion detection method for wireless networks. In this work, a unified weight value is calculated from Received Signal Strength (RSS) and time consumed for RTS-CTS handshake between the sender and receiver.

Ji et al. [28] proposed a centralized algorithm to detect wormholes and show its correctness rigorously. For the distributed wireless network, DAWN, a distributed detection algorithm against wormhole in wireless network coding systems, is proposed by exploring the change of the flow directions of the innovative packets caused by wormholes.

Biswas et al. [29] have proposed a novel wormhole attack detection technique in which node authentication has been used to detect malicious nodes and remove the false positive problem that may arise in wormhole detection techniques. Node authentication not only removes false positive but also helps in mapping exact location of the wormhole and is a kind of double verification for wormhole attack detection.

Patel and Aggarwal [30] projected two-phase detection method for wormhole attack in dynamic sensor networks. This method has a better accuracy rate than most of the existing techniques.

Early approaches proposed for detecting wormhole attacks in wireless ad hoc networks included Packet Leashes [31] and SECTOR [32], which employ concepts of geographical and temporal leashes. The assumption is that each network node knows its exact location, and embeds the location and a timestamp in each packet it sends. If the network is synchronized, then any node that receives these packets can detect a wormhole based on differences in the observed locations and/or calculated times. Such a solution requires a synchronized clock and each node to know its location. The algorithm proposed in this paper does not have these requirements.

More recently, Liu, et al. [33][34] have proposed an anchor-based scheme for detecting several attacks, including wormhole attacks. The scheme uses a hop counting technique to estimate the distance between a node and an anchor node called a “location reference”. Since a wormhole changes the distance from a node to an anchor node, a simple threshold method can be used to determine if the change in distance is caused by a wormhole or by a localization error. The approach also uses a hop counting technique, but it does not involve anchor nodes and, consequently, does not require the manual setup of a sensor network.

A graph-theoretic framework has also been proposed for detecting wormhole attacks [35]. However, this framework relies on “guard nodes,” which are functionally similar to anchor nodes.

WRHT: The Hybrid Wormhole Resistant Technique (WRHT) is a way to detect wormholes in the sensor array using the Delphi concept and watchdog methods. watchdog methods. The value of the number of hops and the probability of a wormhole presence are estimated by each of the source nodes in the network using this method. method. WRHT is an extension of the AODV protocol which aims to detect all categories of wormholes in the network. categories of wormholes in the network using information based on information based on packet loss and packet delay for each hop and also for the entire route in the network [36].

This technique uses the Sinalgo simulator in [15] to efficiently detect the presence of wormholes and increase network security as well as reliability while considering the characteristics and energy constraints of the wireless sensor network. To manage the sensor nodes, the method uses visiting center local (VCL) algorithm to divide the sensor network and form sectors iteratively. A mobile node has been introduced in order to differentiate between the legitimate and malicious nodes with the use of neighborhood discovery of nodes. Upon receiving signals from source nodes, a sink directs the mobile agent to collect information from these nodes present in each sector and summarizes the collected and processed data and finally returns to the sink along with information being collected.

The wormhole geographic distributed detection (WGDD) algorithm is a mechanism to detect wormhole attack without using anchor nodes or specialized hardware. A procedure to count the number of hops of neighboring nodes is used. Once this hop counting process is implemented, a set of hop counts of the neighboring nodes that are one/k hop away is calculated for each of the sensor node. In order to obtain the shortest route, the sensor nodes run the Dijkstra’s algorithm, and then with the help of multi-dimensional scaling, a local map is reconstructed at each of the node. Lastly, in order to detect wormholes in the network, the distortions in the local maps are identified with the help of a novel “diameter” feature [37].

In order to detect wormholes in both uniform and non-uniform environment, a mechanism has been proposed using artificial neural network. This technique is based upon neighborhood count and does not require any specialized hardware. In order to gather neighborhood counts, a node called detector node (which is mobile in nature) travels through random locations in the sensor network. When this detector node enters some location in the sensor network consisting of wormholes, there is a sudden increase in the number of neighbors present and this value is recorded in a data set. Thus, the overall data set contains the neighborhood count in the presence as well in the absence of wormholes in the network, which is in turn fed to the neural network for training and testing purposes. Once testing is over, the presence of wormholes in the sensor network is thus decided by the output of the artificial neural network [38].

A technique to detect and further defend the sensor network from wormhole attack is to use packet leashes. This mechanism imposes a maximum transmission range beyond which transmission of data packets is not allowed. Time delay and geographical location are the constant and independent physical parameters that are used to detect the presence of wormholes in the network. By using time synchronization as well as local information, the packet leashes exercise the maximum transmission range on forwarding of packets so as to prevent wormhole attack. The temporal leash is one type of packet leash where the lifetime of a packet is ensured by an upper bound. While forwarding data packets in a temporal leash, the sender appends the time at which the packet was sent. This value is then compared with the time at which the

packet was received by the receiving node. Another type of leash is the geographical leash which imposes a limit on the distance between the sender and the receiver. The location of the sender as well as the time at which the packet was sent is included in the sent data packet. Computation of the upper bound on the distance between the sender and the receiver is carried out when the data packet reaches its destination [39].
The multi-dimensional scaling visualization of wormhole (MDS-VOW) approach uses the concept of multi-dimensional scaling and visualization to detect wormholes present in the wireless sensor network. Firstly, the outline of the wireless sensor network comprising the sensor nodes is reconstructed using multi-dimensional scaling. The distance between each pair of sensor nodes is evaluated by providing the imprecise space between the sensor nodes that can hear each other as inputs, and thus, a virtual position for all the nodes is estimated. While estimating the distance, few errors occur in the reconstructed network whose adverse effects are minimized by using a surface smoothing technique. Finally, an analysis of the reconstructed network is carried out so as to detect the fake neighbors present in that network [40].

In order to mitigate wormhole attack, this technique prevents malicious nodes from creating false neighbors with the help of directional antennas. Since wormhole attack cannot be launched if the wormhole link is detected as fake and its requests are neglected, therefore a precise set of neighboring nodes is maintained for each of the sensor nodes. On the basis of the signals received, direction information can be collected by a sensor node using the directional antennas. Three protocols are designed in this approach that uses directional information to counter wormhole attack [41].

Transmission Range-Based Method (TRM) technique used to efficiently detect wormhole attack without the need of any additional hardware. It uses the local neighborhood information to determine a network affected by wormhole attack, even in the presence of large transmission range. The TRM uses a directed graph with "N" sensor nodes to represent the network model. The malicious nodes and the normal nodes are categorized into two types and can be differentiated in terms of power, transmission range, and capability of computation. The network topology between two sensor nodes within a certain communication range is analyzed in order to detect wormholes between them with the help of geometric relationship of the nodes' location [42].

In [43] authors Use the concepts of range-free localization, two methods have been proposed in this paper in order to detect wormholes in the wireless sensor network. A scheme called "sensor localization with ring overlapping based on comparison of received signal strength indicator" (ROCRRSI) has been used as a range localization process for detection of wormholes in the network. The two methods that have been developed observe the irregularity in the network measurements at the physical layer and analyze the RSS value estimated by the nodes involved in localization process. The first strategy is implemented while the localization procedure is carried out by the sensor nodes, while the second strategy is implemented once the localization procedure has been done by the nodes.

The distributed technique detects the presence of wormhole attack in multi-hop wireless networks based on connectivity information [44]. This is a localized algorithm wherein the wormholes are detected by locating forbidden structures in the connectivity graph of the network. The algorithm is developed with the help of a unit disk graph model and a general communication model where the communication model can be known or unknown. The basic idea is to locate structures in the graph that does not belong to a legitimate connectivity graph as embedding of the unit disk graph is not allowed by these illegal substructures. Although for all cases the algorithm will not be able to detect the wormhole attack, for connected networks, it guarantees a high detection accuracy.

An approach for detecting wormhole attack has been proposed in the [45]. paper by analyzing the number of packets that have been sent and received by the sensor nodes in the network. The method is divided into two phases where the first phase is to generate keys and the second one is to detect wormholes in the network. In the first phase, the generation of a secret key is carried out in order to prevent alteration of data by the illegitimate nodes. Once each of the sensor node locates their geographic location, they use a HELLO message to acquire information regarding neighboring sensor nodes that are one hop away. The second phase emphasizes on gathering data from the sent and received packets of each of the sensor nodes. This gathered data is then validated so as to detect the presence of wormhole attack in the sensor network.

Neighborhood and Connectivity Information: In this approach, a protocol has been proposed in order to detect wormhole attack on the basis of neighborhood and connectivity information. With the use of a key management protocol that is secure, pre-distributive, and pair-wise in nature, this method is able to detect wormhole attack effectively for a minimal storage cost. There are three phases of the proposed method, out of which the first phase is to build the neighborhood table comprising of neighbors that are one hop away for each of the sensor nodes present in the network. The neighborhood table is extended to include the neighboring nodes that are two hops away during the second phase. The process of detecting the wormhole attack is carried out in the last phase. This detection procedure can be used with wireless sensor networks having constraints in resources [46].

Neighbor Discovery and Path Verification: This wormhole detection and prevention procedure are able to detect and also defend the presence of wormhole attack in the AODV protocol of the sensor network by discovery of neighboring nodes and verification of the paths taken by the sensor nodes. In order to make this algorithm work, a secure communication is established between the source and the destination nodes. The first phase of the approach is to discover routes of neighboring nodes where a HELLO message is shared among the neighboring nodes so that at each level, packets can be encrypted. In the second phase, a list of neighbors with one hop and two-hop transmission range is created so as to perform verification of the neighboring nodes in the network. The sensor network is said to be affected by the wormhole attack if there is an illegal entry of neighboring nodes that are two hops away [47].

In [48] the authors design SeT-D2D (Secure and Trust D2D), according to which trustworthiness inferred from both direct interactions and social-awareness parameters is exploited to properly select relay nodes. Main contributions of our research consist in the introduction of a model for the assessment of network nodes' trustworthiness and the implementation of security mechanisms to protect the data transmitted in D2D communications and the privacy of the

involved users. The conducted simulation campaign testifies to the ability of the proposed solution to effectively select relay nodes, which leads to an improved network performance.

Packet forwarding in multi-hop wireless ad hoc network is a cooperative task, in which intermediate nodes participate voluntarily to deliver packets to the destination node. An intermediate node can behave selfishly or maliciously to drop packets going thought it, instead of forwarding them to its successor. This misbehaving can be called Black hole attack. The motivation of the dropper node is the preservation of its resources like its limited energy, or the launch of a denial of service attack. The consequence of such attack is node's isolation and network performance degradation [48]-[51].

The [53] presents a novel Moving-target Defense (MtD) to enhance the channel secrecy capacity in a Decode-and-Forward (DF) dual-phase large network containing K relays and source nodes with multi-antennas operating on different frequencies. Our MtD approach enables multidimensional **spatiotemporal** diversification for the user's traffic in cooperative wireless transmission, to obfuscate signal transmission-patterns and data, across the entire spectrum available. In **time**, we obfuscate the transmitted data by employing real-time shuffling between real and fake data. In **space**, we enforce real-time hopping between multiple frequencies to evade signal tracing. The authors examine the ergodic channel secrecy capacity considering two behavioral patterns; cooperative and uncooperative untrustworthy-relays.Simulation results showed that, for a powerful malicious user with multiple access points, and no pre-knowledge of the diversification patterns used by the system, it is very hard to eavesdrop a meaningful portion of the signal or the data stream.

VI. Wormhole Detection Algorithm

As previously mentioned, each node in the network has to select a set of one-hop neighbors MPR set, which is constructed by the smallest number of nodes that allow the MPR selector to cover every two-hop neighbor through, at least one of its MPRs.

To deal with a Worm Hole attack, we propose an algorithm to select MPR with additional coverage without giving priority to nodes with higher willingness. The aim of this algorithm is to reduce the impact of malicious nodes trying to be selected as MPR nodes.

Our approach is a modified version of the RFC 3626 [3] MPR coverage parameter which allows increasing the number of nodes through which, the MPR selector can reach every two hop neighbor. For example, if MPR-Coverage is equal to K it means that, if possible every two-hop neighbor can be reached though at least K nodes (K=1, standard OLSR).

Before introducing this algorithm, some notations should be described first:

1HN_set(X): the set of node X's one hop symmetric neighbors. It is created by the way of changing HELLO messages between nodes.

2HN_set(X): the set of node X's two hop symmetric neighbors excluding any node in 1HN_set(X). It is also created by the way of exchanging HELLO messages.

MPR_set (E): the set of nodes selected as MPR by the node E. (MPR_set (E) ⊆ 1HN_set (E)).

MPRS_set (E): the set of symmetric neighbours which have selected the node E as MPR. (MPRS_set (E) ∈ 1HN_set (E)).

Degree (X, Y): the degree of node X's one hop neighbor; returns the number of nodes in 2HN_set(X) such that {2HN_set(X) ∩ 1HN_set(Y) ≠ Ø } assuming that Y ∈ 1HN_set(X).

Reachability (X, Y): the number of nodes in 2HN_set(X) which are not yet covered by at least one node in the MPR_set(X), and which are reachable through node Y.

Poorly_set: A subset of 2NH_set(X) which is covered by less than K nodes in 1NH_set(X).

Well_set: A subset of 2NH_set(X) which is covered by more than K nodes in 1NH_set(X).

The proposed heuristic for selecting MPRs, by each node, is then as follows:

1) Calculate degree of each node in one hop neighbour of X.
2) Select as MPRs those nodes in one hop neighbor which cover the poorly covered nodes in two hop neighbors.
3) Remove the poorly covered nodes from two hop neighbor set for the rest of the computation process.

While there exist nodes in two hop neighbor which are not covered by at least k nodes in the MPR set.

a) Calculate the reachability of each node in 1HN_set(X) not in MPR_set.
b) Select as MPR the node which provide reachability to the maximum number of nodes in 2HN_set(X) and maximum degree.
c) Eliminate all nodes in 2HN_set(X) now covered by at least, K node in the MPR_set.

The pseudo code of the proposed approach is listed below.

Degree(X, Y)

foreach *Y ∈1HN_set(X)* ***do***
    D ← ***0 ;***
    D ← ***CARD*** *{1HN_set(Y) \ {1HN_set(X) \ {X,Y}}};*
Return D ;

Poorly_set(X)

P ← ***Ø ;***
For each *Y ∈2HN*_set(X)* ***do***
    If CARD *{1HN_set(Y) ∩ 1HN*_set(X) } < K* ***then***
        P ← P ∪{Y} ;
        *MPR_set(X) ← MPR_set(X) ∪{1HN*_set(X) ∩ 1HN_set(Y) } ;*
    *2HN*_set(X) ← 2HN*_set(X) \ {Y} ;*
P ← *Poorly_set(X);*

```
Return (P);

Reachability (X, Y)
For each Y ∈1HN*_set(X) do
    R ← 0 ;
    R ← CARD {{F / F ∈2HN*_set(X) ∩ 1HN_set(Y) and
            MPR_set(X) ∩ 1HN_set(F) = Ø }} ;
Return R;

Well_Set (X)
W ← Ø ;
For each (Z ∈2HN*_set(X)
    If ( CARD {1HN_set(Z) ∩ MPR_set(X)}) >= K) do
        2HN*_set(X) ← 2HN*_set(X) \ {Z}
        W← W ∪{Z}
Return (W);

MPR_SET (X)
1HN*_set(X ) ← 1HN_set(X) ;
2HN*_set(X) ← 2HN_set(X) ;
MPR_set (x) ← Ø ;
Poorly_Set(X) ;
Well_Set (X);
For all node Y ∈1HN_set(X) do
    Degree(X, Y) ;
While (Well_Set (X) ≠ Ø) do
    For each Y ∈1HN*_set(X) do
        Reachability (X, Y);
    If ( Reachability (X,Y)= Max { Reachability (X,Y),
                                   Y ∈1HN*_set(X)}
        and Degree(X,Y) = Max { Degree (X,Y), Y ∈
        1HN*_set(X)} )then
        MPR_set(X) ← MPR_set(X) ∪{Y} ;
        Well_Set (X)← Well_Set (X) \ {Y};
    Return ← MPR_set (X)
```

The function Degree (X, Y) return a number of a 1-hop neighbor node y is defined as the number of symmetric neighbors of node y, excluding all the members of 1-hop neighbor and excluding the node performing the computation. the number of nodes in 2HN_set(X) which are not yet covered by at least MPRS_Coverage nodes in the MPR_set, and which are reachable through this 1-hop neighbor are calculated by the function Reachability (X,Y).

A poorly covered node is a node in 2HN_set(X) which is covered by less than MPRS_Coverage nodes in 1HN_set(X). On the other hand, the function Well_Set() returns the two-hop nodes which are covered by a number greater than MPRS_Coverage.

VII. Simulation Model

To test the effectiveness of our solution, simulations were implemented using network simulator NS3 [52] with modified version of the OLSR implementation. We integrated our scheme in implemented OLSR protocol for the detection of the Worm hole attack. All OLSR protocol default values from [3] were used (Table 2). Simulations were performed for 25-100 nodes with a transmission range of 200 meters, in an area of size 1500*1500 meters during 200 seconds. Random waypoint model is used as the node mobility model with nodes speed of 20 m/s. The number of malicious nodes is varied from 0 to 5 (Table 3).

In our experiments, we assume that all nodes have the same characteristics. Thus, every node has just one interface and all links connecting nodes have that same Willingness in order to carry and forward traffic on behalf of other nodes, except for those that have been selected as misbehaving nodes (Table 2). Scenario 1 simulates a standard protocol without attacks while scenario 2 simulates our proposed approach Resilient-OLSR and studies its performances in the case of a Worm Hole attack. We propose to study these performances via Packets Delivery Ratio, End To End Delay, Throughput and Average of MPR nodes.

Figure 5. Compares standard OLSR to our proposed approach with K_coverage. We observe that in the presence of the attack, the PDR in K_coverage=1 is very low. The only packets received by the node are the ones received before launching the attack. Furthermore, we observe that the PDR increases when node speed increases. The reason is that, when the destination node moves rapidly, it has more chances to select node as MPR other than the victim node.

On the other hand, when the New-OLSR is under attack, the PDR is better than a standard OLSR under attack. The reason is that; in K_coverage = 2 the source node has (if possible) two alternatives to reach its two hop Neighbors. If one of them is a misbehaving node the Dijkstra algorithm can select the route connecting a given source and destination nodes which not content this misbehaving node.

Parameter	description
Simulator	NS-3.
Connection type	CBR/UDP
Simulation area	1500x1500
Transmission range	200m
Mobility Model	Random WayPoint
Packet size	2048 bytes
Density	25,50,70,100
Malicious nodes	0-5
Duration	200s
Pause Time	0s
Attack start	10s

Table 2. Simulation Parameters

Parameter	Values
TC interval	5 s
HELLO interval	2 s
Refresh Timout Interval	2 s
Neighbor hold time	6 s
Topology hold time	15 s
K-Coverage	1-2
Duplicate hold time	30 s

Table 3. OLSR Parameters

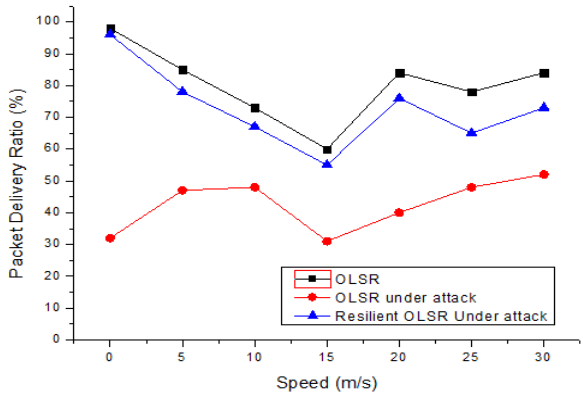

Figure 5. Packets Delivery Ratio VS Speed.

Figure 6. Shows the end-to-end delay of the two studied protocols. OLSR has the lowest end-to-end delay at low and high mobility due to the proactive routing approach of OLSR protocol; every node in the network has route to any possible destination in its routing table at any given time. Data received from the upper transport layer are immediately transmitted, as a route to the destination is already in the node's routing table. On the other hand. Our approach requires more time because of the overhead caused by the increase in MPR nodes, which will generate and transmit TC messages.

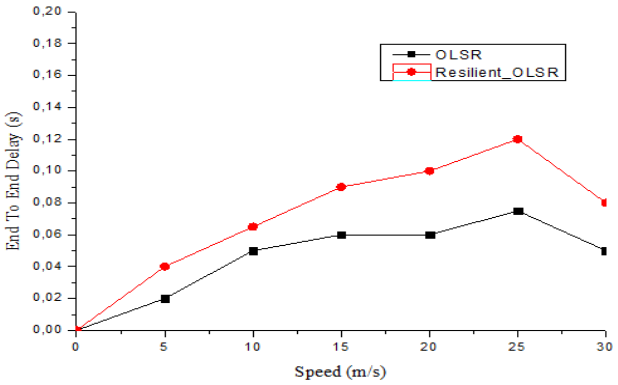

Figure 6. End To End Delay Vs Speed

Figure. 7 shows the delay depending on the packets transmitted for OLSR and Resilient_OLSR. The packet delay is less than 500 ms between transmission 300 and 650 and the peak value 975 ms is reached at 700 transmissions. After analyzing the graph, the packet delay in the OLSR approach is approximately 78%.

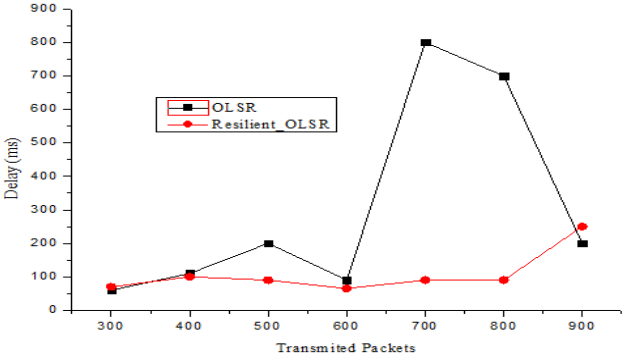

Figure 7. Delay VS Transmited Packets

In Figure 8. We notice that the throughput of our approach is better than OLSR under attack but when we increase the number of attackers we notice a degradation of the throughput for both protocols.

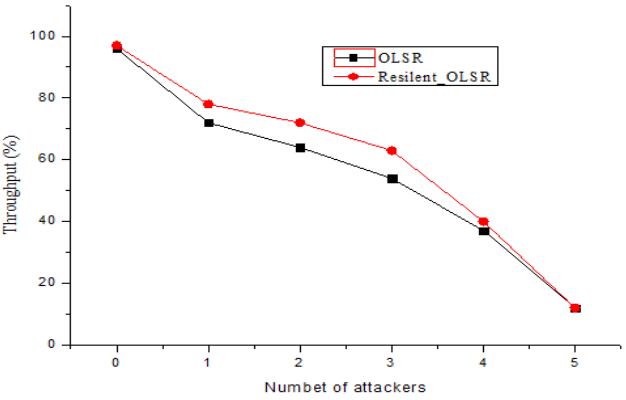

Figure 8. Throughput VS Numbers of attacker nodes

Figure 9. Gives the average number of MPR nodes selected by OLSR and Resilent_OLSR for different densities. We can see that density clearly affects the number of MPR node selected by both protocols. It increases when density is increased while the number of MPR nodes selected by OLSR is less than the number selected by our approach. The reason is that our

selection algorithm extends network knowledge by additional coverage.

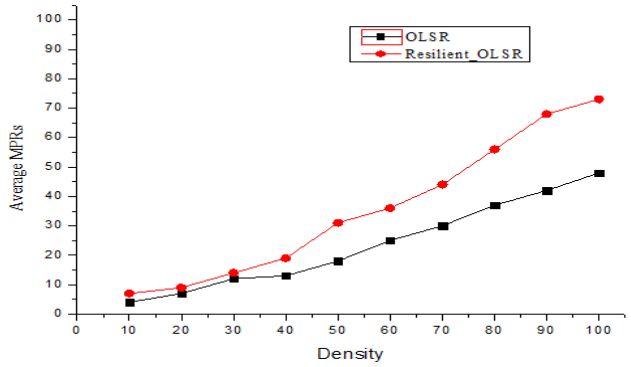

Figure 9. Average of MPR nodes VS Density

Figure 10. Depicts our results, but with one to five misbehavior nodes. Again, we observe that our approach gates the effect of misbehaving nodes with a better performance than the standard protocol.

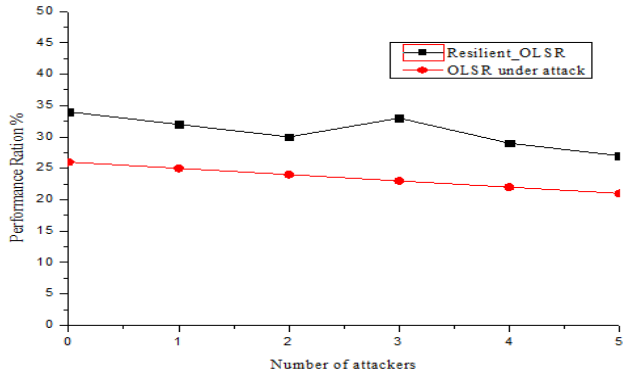

Figure 10. Performance Ratio VS Number of attacker nodes

VIII. Conclusion

Routing in ad hoc networks is an extremely important process whose objective is to allow the routing of user data between all the nodes that make up the network. Therefore, it is of utmost importance to protect it against any kind of attacks, voluntary or not. However, the constraints related to the absence of centralized management infrastructures, the use of wireless communication channels and the limited protection of nodes, as well as the lack of inter-node cooperation, make this task very delicate.

Wormhole attack forms a tunnel to relay packets among malicious nodes. This type of attack can affect the topology construction mechanism especially in the case of proactive routing protocols such as OLSR. In this paper, we have proposed a new way to protect network from wormhole attack by proposing a novel approach to select MPR nodes by additional coverage. This gives priority to a node that covers maximum nodes in two hop neighbors which do not show strong characteristics to influence the MPR selection to be selected as MPR.

This technique allowed the nodes in the network to have other alternatives to transmit TC control messages and, thus, increase the accuracy of the topological knowledge maintained by each mobile node in the network.

Simulation results show that the proposed approach is better than existing ones in terms of packet delivery ratio, throughput, end to end delay and topology knowledge which provides significant benefits for communication protocols. This additional knowledge may support the construction of more robust routing paths, or event multipath, in order to provide security.

Moreover, in the continuity of the present work, we consider to remedy the problem of suppression of control messages and the non-cooperation of nodes, by displaying a selfish behavior. We propose to look for a solution that spreads over a model that takes into consideration the different layers of the OSI model, and the different parameters specific to each layer, notably the Signal to Noise Ratio, the reception power for the physical layer, the control packets and acknowledgments for the MAC layer and of course the OLSR routing protocol specifications at the network layer. This approach will certainly limit the number of false alarms.

References

[1] Perkins C, Belding-Royer E, Das S. Ad hoc on-demand distance vector (AODV) routing. IETF RFC 3561, (2003).

[2] Johnson DB, Maltz DA, Hu Y-C. The dynamic source routing protocol for mobile ad hoc networks (DSR). IETF Internet Draft, draft-ietf-manet-dsr-09, (2003).

[3] T. Clausen, C. Dearlove, P. Jacquet, U. Herberg. IETF 7181 The Optimized Link State Routing Protocol OLSRV2, April (2014).

[4] C.E. Perkins and P. Bhagwat, "Highly dynamic destination-sequenced distance vector routing (DSDV) for mobile computers," in Proc. ACM SIGCOMM 94, pp. 234-244, London, UK, Oct. (1994).

[5] M.-Y. Su, "WARP: A wormhole-avoidance routing protocol by anomaly detection in mobile ad hoc networks," Computers & Security, vol. 29, pp. 208–224, Mar. (2010).

[6] R. Stoleru, H. Wu, and H. Chenji, "Secure neighbor discovery and wormhole localization in mobile ad hoc networks," Ad Hoc Networks, vol. 10, pp. 1179–1190, Sept. (2012).

[7] Deborah E, Ramesh G, John H, Satish K. Next century challenges. Scalable coordination in sensor networks. In MOBICOM, pages 263–270, 1999.

[8] Robert M, John J, M. Frans K, Jinyang L, Douglas, C. A scalable ad hoc wireless network system. In ACM SIGOPS European Workshop, pages 61–65. ACM, 2000.

[9] 802.11a: High-speed Physical Layer in the 5 GHz band. http://standards.ieee.org/getieee802/download/802.11a-1999.pdf, 1999.

[10] 802.11b: Higher speed Physical Layer (PHY) extension in the 2.4 GHz band. http://standards.ieee.org/getieee802/download/802.11b-1999.pdf, 1999.

[11] 802.11g: Further Higher-Speed Physical Layer Extension in the 2.4 GHz Band. http://standards.ieee.org/getieee802/download/802.11g-2003.pdf, 2003.

[12] 802.11n: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Enhancements for Higher Throughput, IEEE std 802.11n, 2009.
[13] Xu, Y., Chen, G., Ford, J. and Makedon, F., in IFIP International Federation for Information Processing, Volume 253, Critical Infrastructure Protection, eds. E. Goetz and S.Shenoi; (Boston: Springer), pp. 267–279. (2008).
[14] Bendjima, M., Feham, M.: Wormhole attack detection in wireless sensor networks. In: Proceedings of SAI Computing Conference, London, UK, 13–15 July 2016
[15] Maidamwar, P., Chavhan, N.: A survey on security issues to detect wormhole attack in wireless sensor network. Int. J. AdHoc Netw. Syst. 2(4), 37–50 (2012)
[16] Pawar, R.B., Patil, P.U., Bombale, G., Zalani, A.: Wormhole attack and it's variants in wireless sensor network: a survey. Int. J. Eng. Res. Technol. 3(8), 1176–1179 (2014)
[17] Singh, R., Singh, J., Singh, R.: WRHT: a hybrid technique for detection of wormhole attack in wireless sensor networks. Mobile Inf. Syst. 8354930, 13 (2016)
[18] Poonam, M.: Wormhole attack in wireless sensor network: a survey. Int. J. Adv. Res. Sci. Eng. 5(2), 110–117 (2016)
[19] Gupta, A., Gupta, A.K.: A survey: detection and prevention of wormhole attack in wireless sensor networks. Glob. J. Comput. Sci. Technol.: E Netw. Web Secur. 14(1), 23–31 (2014)
[20] Ladva, M.M., Lathigara, A.M.: Wormhole attack detection and prevention technique in mobile ad-hoc network: a review. Int. J. Innov. Emerg. Res. Eng. 2(2), 83–88 (2015)
[21] Ughade, S., Kapoor, R.K., Pandey, A.: An ov*erview on wormhole attack in wireless sensor network: challenges, impact and detection approach. Int. J. Recent Develop. Eng. Technol. 2(4), 105–110 (2014)
[22] W. Wang, B. Bhargava, Y. Lu, and X. Wu, "Defending against wormhole attacks in mobile ad hoc networks," Wireless Communications and Mobile Computing, vol. 6, no. 4, pp. 483–503, (2006).
[23] Y. Zhang, W. Liu, W. Lou, and Y. Fang, "Location-based compromise-tolerant security mechanisms for wireless sensor networks," IEEE Journal on Selected Areas in Communications, vol. 24, no. 2, pp. 247–260, (2006).
[24] I.Khalil, S. Bagchi, and N. B. Shroff, "LITEWORP: a lightweight countermeasure for the wormhole attack in multihop wireless networks," in Proceedings of the International Conference on Dependable Systems and Networks (DSN '05), pp. 612–621, Yokohama, Japan, June (2005).
[25] I. Khalil, S. Bagchi, and N. B. Shroff, "Mobiworp: mitigation of the wormhole attack in mobile multihop wireless networks," in Proceedings of the IEEE Secure Communication, pp. 1–12, September (2006).
[26] N. Song, L. Qian, and X. Li, "Wormhole attacks detection in wireless ad hoc networks: a statistical analysis approach," in Proceedings of 19th IEEE International Parallel and Distributed Processing Symposium (IEEE IPDPS '05), p. 289, Denver, Colo, USA, April (2005).
[27] Singh, Jatinder & Kaur, Lakhwinder & Gupta, Savita. A Cross-Layer Based Intrusion Detection Technique for Wireless Networks. International Arab Journal of Information Technology. (2012)
[28] S. Ji, T. Chen, and S. Zhong, "Wormhole attack detection algorithms in wireless network coding systems," IEEE Transactions on Mobile Computing, vol. 14, no. 3, pp. 660–674, (2015).
[29] J. Biswas, A. Gupta, and D. Singh, "WADP: a wormhole attack detection and prevention technique in MANET using modified AODV routing protocol," in Proceedings of the 9th IEEE International Conference on Industrial and Information Systems (ICIIS'14), pp. 1–6, December (2014).
[30] M. Patel and A. Aggarwal, "Two phase wormhole detection approach for dynamic wireless sensor networks," in Proceedings of the IEEE International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET '16), pp. 2109–2112, Chennai, India, March (2016).
[31] Y. Hu, A. Perrig and D. Johnson, "Packet leashes: A defense against wormhole attacks in wireless networks", Proceedings of the Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies, vol. 3, pp. 1976 – 1986,(2003).
[32] S. Capkun, L. Buttyan and J. Hubaux, "SECTOR: Secure tracking of node encounters in multi-hop wireless networks", Proceedings of the First ACM Workshop on Security of Ad Hoc and Sensor Networks, pp. 21 – 32, (2003).
[33] Y. Cho, G. Qu, and Y. Wu, "Insider threats against trust mechanism with watchdog and defending approaches in wireless sensor networks," in Proceedings of the 1st IEEE Security and Privacy Workshops (SPW '12), pp. 134–141, May (2012).
[34] D. Liu, P. Ning and W. Du, Attack-resistant location estimation in sensor networks", Proceedings of the Fourth International Symposium on Information Processing in Sensor Networks, pp. 99 – 106, (2005).
[35] Singh, R., Singh, J., Singh, R.: WRHT: a hybrid technique for detection of wormhole attack in wireless sensor networks. Mobile Inf. Syst. 8354930, 13 (2016)
[36] Xu, Y.,Chen, G., Ford, J., Makedon, F.: Detecting wormhole attacks in wireless sensor networks. In: Goetz, E., Shenoi, S. (eds) Critical Infrastructure Protection. International Federation for Information Processing, pp. 267–279. Springer Series in Computer Science, Springer, Berlin (2008)
[37] Shaon, M.N.A., Ferens, K.: Wireless sensor network wormhole detection using an artificial neural network. In: International Conference of Wireless Networks, pp. 115–120, Las Vegas, USA (2015)
[38] Hu, Y.C., Perrig, A., Johnson, D.B.: Wormhole attacks in wireless networks. IEEE J. Sel. Areas Commun. 24(2), 370–380 (2006)
[39] Wang, W., Bhargava, B.: Visualization of wormholes in sensor networks. In: Proceedings of 3rd ACM workshop on wireless security (WiSe'04), pp. 51–60. Philadelphia, USA (2004)
[40] Hu, L., Evans, D.: Using directional antennas to prevent wormhole attacks. In: Proceedings of Network and

Distributed System Security Symposium (NDSS 2004), San Diego, California, USA (2004)
[41] Wu, G., Chen, X., Yao, L., Lee, Y., Yim, K.: An efficient wormhole attack detection method in wireless sensor networks. Comput. Sci. Inf. Syst. 11(3), 1127–1141 (2014
[42] García-Otero, M., Población-Hernández, A.: Detection of wormhole attacks in wireless sensor networks using range-free localization. In: Proceedings of 17th International Workshop on Computer Aided Modelling and Design of Communication Links and Networks (CAMAD), pp. 21–25, Barcelona, Spain (2012)
[43] Maheshwari, R., Gao, J., Das, S.R.: Detecting wormhole attacks in wireless networks using connectivity information. In: Proceedings of 26th IEEE International Conference on Computer Communications, Barcelona, Spain (2007)
[44] Buch, D., Jinwala, D.: Detection of wormhole attacks in wireless sensor network. In: Proceedings of International Conference on Advances in Recent Technologies in Communication and Computing, pp. 7–14, Bangalore, India (2011)
[45] Patel, M., Aggarwal, A.: Detection of hidden wormhole attack in wireless sensor networks using neighbourhood and connectivity information. Int. J. Ad hoc Netw. Syst. 6(1) (2016)
[46] Johnson, M.O., Siddiqui, A., Karami, A.: A wormhole attack detection and prevention technique in wireless sensor network. Int. J. Comput. Appl. 174(4), 1–8 (2017)
[47] C. Suraci, S. Pizzi, D. Garompolo, G. Araniti, A. Molinaro, A. Iera,Trusted and secured D2D-aided communications in 5G networks,Ad Hoc Networks journal,Volume 114, 2021
[48] Zougagh H., Idboufker N., El Mourabit Y., Saadi Y., Elouaham S. (2021) Avoiding Wormhole Attack in MANET Using an Extending Network Knowledge. In: Abraham A., Sasaki H., Rios R., Gandhi N., Singh U., Ma K. (eds) Innovations in Bio-Inspired Computing and Applications. IBICA 2020. Advances in Intelligent Systems and Computing, vol 1372. Springer, Cham. https://doi.org/10.1007/978-3-030-73603-3_20
[49] Zougagh, H., Toumanari, A., Latif, R., & Idboufker, N. (2015). A novel security approach for struggling black hole attack in optimised link state routing protocol. International Journal of Sensor Networks, 18(1–2), 101–110.
[50] Zougagh, H., Idboufker, N., Zoubairi, R., El Ayachi.,R. (2019). Prevention of Black Hole Attacks on Mobile Ad Hoc Networks Through Intrusion Detection Systems. International Journal of Business Data Communications and Networking (IJBDCN) 15, 2 (2019), 73–91.
[51] M. Ghourab, M Azab, Benign false-data injection as a moving-target defense to secure mobile wireless communications, Ad Hoc Networks, Volume 102, 2020.
[52] The Network Simulator. ns-2. http://www.isi.edu/nsnam/ns/. Last accessed 2020/6/20

Author Biographies

Hicham Zougagh is a PhD degree in telecommunication and Computer Science from the university of Cadi Ayyad. He is currently a full Professor at the Faculty of Sciences and Techniques of Beni Mellal belonging to the University Moulay Slimane since May 2016, Hicham Zougagh is a part of computer sciences department. He is also a member of TIAD laboratory. His recent interest is in the security, routing protocols, QOS in ad hoc networks, sensor networks, Vanets, IoT and IA

Noureddine Idboufker is a Ph.D. degree in Telecommunications and Computer Science from the University of Chouaib Doukkali. He is currently a full Professor at the National School of Applied Sciences of Marrakech belonging to the University Cadi Ayyad. Since June 2006, Noureddine Idboufker is a part of the Telecommunications and Computer Sciences Department. He was also assistant director of TIM laboratory where he is a supervisor of research activities. From 1996 to June 2006, he was working at the R&D department of Maroc Telecom as an R&D engineer. He has worked on several projects, especially in the IP field. During this period, he has been the head of team of the MPLS, QoS and NGN projects. His main research includes evolutionary computation, constrained based routing and Quality of service. His recent interest is in the evaluation of QoS, QoE, Security in SDN, routing and security in Mobile Ad Hoc Network plus IT service Governance.

Rachid Elayachi received a Ph.D degree in signal processing in 2012 and the habilitation degree in 2017, from Moulay Slimane University, Morocco. Currently, he is a Professor with the Department of computer sciences, Moulay Slimane University, Beni Mellal, Morocco. His research interest is in information treatment, mac hine learning…

Youssef Saadi is currently a computer science assistant professor at Faculty of Sciences and Technologies, Sultan Moulay Slimane University, Béni Mellal, Morocco. He joined Faculty of Sciences and Technologies in september 2018. He is teaching graduate and undergraduate courses in the areas of object-oriented design, object-oriented programming, performance modeling and analysis, Cloud Computing and Project Management. His current research interests managing cloud resources for green IT, sckeduling tasks for resource usage optimization and wireless multi hop networks performance improvement and evaluation. He serves also as scientific committee member in many international and peer-reviewed conferences.

Samir Elouaham received the Ph.D degree in signal processing in 2014 from Ibn Zohr University, Morocco.
Currently, he is a Professor with the Department of physic, Chouayb Doukkali University, Eljadida, Morocco. His research interests include biomedical signal processing, fuzzy logic, time-frequency signal processing and he is working on the modeling, filtering, and analysis of fetal cardiac signals.

Azzedine Dliou was born in Agadir, Morocco, on June 30, 1982. He received the D.E.S.A degree in mathematical and computer from Ibn Zohr University, Agadir, Morocco in 2007. received the Ph.D degree in signal processing in 2014 from Ibn Zohr University, Morocco.
Currently, he is a computer sciences professor at Faculty faculty of applied sciences Ibn Zohr University, Agadir, Morocco. His research interests include biomedical signal processing, fuzzy logic, time-frequency signal processing and he is working on IA, Deep learning, Security.