Shapiro-Wilk Test to Detect The Routing Attacks In MANET

Abdellah Nabou (a.nabou@ensem.ac.ma)
RITM Laboratory ENSEM,EST HASSAN II University of Casablanca https://orcid.org/0000-0003-2119-1638

My driss Laanaoui
Cadi Ayyad University: Universite Cadi Ayyad

Mohammed Ouzzif
Hassan II University of Casablanca

Mohammed Alamine El houssaini
Chouaib Doukkali University: Universite Chouaib Doukkali

Research Article

Keywords: MANET, OLSR, Active Routing Attacks, Security, Shapiro-Wilk

Posted Date: June 2nd, 2021

DOI: https://doi.org/10.21203/rs.3.rs-473896/v1

Shapiro-Wilk Test to Detect the Routing Attacks In MANET

Abdellah Nabou [a], My Driss Laanaoui [b] ,Mohammed Ouzzif [a]
and Mohammed-Alamine El Houssaini [c]
[a] RITM Laboratory, CED Engineering Sciences, EST, ENSEM
Hassan II University of Casablanca, Morocco
*a.nabou@ensem.ac.ma, oussif@gmail.com
[b] Laboratory LIIS, University Cadi Ayyad
d.laanaYes@uca.ma
[c] ESEF Chouaib Doukkali University of El Jadida, Morocco
elhoussaini.m@ucd.ac.ma

Abstract. In the last recent years, the number of wireless devices has been growing and the security challenges increases too. Mobile Ad hoc Network (MANET) considers as a part of wireless network that connects mobile devices by using wireless channels without infrastructure. MANET use specific protocols to ensure the connectivity and exchange data between the source and destination. Optimized Link State Routing Protocol (OLSR) is a table-driven protocol that keep the route to all destination at any times, unfortunately it can be affected by many active routing attacks that reduce its performance by dropping the exchange packets or stopping the forward of data. In this paper we present a new approach to detect any active routing attacks by using the concept of Shapiro-Wilk test. Our method of detection is easy to implement and does not require any modification in the standard version of OLSR routing protocol as we will demonstrate by NS-3 simulations the detection of Black hole, Worm hole and Node isolation attacks that consider as most known attacks in MANET. A real experience is done by creating a small ad hoc network that connect six wireless devices by using OLSR protocol and finally we detect the presence of an active routing attack by applying our proposed method.

Keywords: MANET; OLSR; Active Routing Attacks; Security; Shapiro-Wilk

1. Introduction

MANET is constructed by wireless devices called by nodes without any fixed infrastructure. The main supposition considered in MANET is that all devices are trusted nodes. However, some of them can be malicious nodes and therefore can drop or stop forwarding the data packets to the destination node [1]. OLSR routing protocol considers as the most popular proactive MANET protocol thanks to its new concept MultiPoint Relay (MPR) which are selected nodes neighbors from 1-hop neighbor to reach 2-hop neighbor used for forwarding the data packets in the network [2]. In the other meaning, the MPRs nodes are selective devices that forward broadcast messages during the flooding process [3]. The basic idea of MPRs is to decrease the overhead of flooding messages by limiting redundant relays in the same area of the network. This mechanism reduces the network overhead compared to the classical flooding and make OLSR as well the most appropriate MANET routing protocol for high density. The assumption of trusted nodes and the transparence in OLSR algorithms for selection the MPR nodes, added to other constraints of MANET as mobility, infrastructure-less and energy consumption, all these factors make OLSR protocol more vulnerable to many attacks that reduce it performance. In literature, the MANET routing attacks are classified into two types, based on the nature of attack: passive and active attacks in follow we cite the difference between them [4]:

- Passive attack is of eavesdropping in nature like passive listening of communication without any intervention, the attackers spy on the data exchanged in the network without modification. The detection of passive attacks is difficult because the routing protocol itself is not affected.
- Active attack is an attack which involves modifications or insertion of control or routing messages during communications. The active attack may decrease the efficiency of any MANET routing protocol by dropping or stop forwarding data packets to the destination.

In this paper we present new efficient method to detect any active routing attacks can affect the performance of OLSR routing protocol. Our proposed method reckons on Normality Test by using Shapiro-Wilk method [5] that considers as effeteness and powerful for the small number of sample size s ($s \leq 50$) [6]. To test the effeteness of this method, we simulated OLSR routing protocol under three different MANET active routing attacks which are: The Black hole attack, the Worm hole attack and the Node Isolation Attack. According to our modest knowledge of the state of the art, this technique has not been used before for the detection of routing attacks in MANET. To test the effeteness of our proposed method in real environment, we create a small ad hoc network by connecting 6 wireless devices (three personnel computers and three smartphones) and we configure them to use OLSR as MANET routing protocol, we integer the Node Isolation attack that does not require more devices, the results obtained by our proposed method confirm the detection of this active routing attack in MANET.

The remainder of the paper is organized as follows: Sect. 2 present OLSR routing protocol followed by MANET active routing attacks in Sect. 3. Sect 4 simply surveys the related works. Sect. 5 introduces the basic idea of our proposed method of detection. Sect. 6 describes simulations and results, and finally Sect. 7 draws the conclusions.

2. OLSR routing Protocol

OLSR is a proactive routing protocol for mobile ad hoc networks, it uses the link state algorithm that calculates routes based on the cost of the path. In traditional link-state routing algorithms, each node broadcasts its direct links to its neighbors throughout the network, whereas OLSR minimizes the traditional flooding of control traffic by selective flooding using a node called a multipoint relay (MPR) to relay control messages (Figure 1).

With this technique, only nodes selected as MPRs (nodes with gray color) are allowed to retransmit the periodic control messages necessary to maintain routes to all destinations in the network [7].

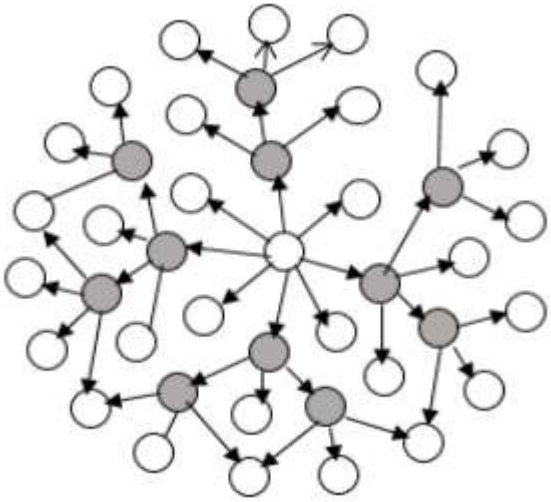

Fig. 1. Flooding by the technic of MPRs in OLSR4

MPR nodes reduce the number of duplicate packets distributed on the network and only they are authorized to broadcast control messages, the other nodes use these messages to construct their global network vision. Each node selects its MPR from its symmetric set to achieve its neighbors with two hops [8].

The protocol is especially useful for large and dense networks, as optimization using MPR performs well in this environment. The higher the network, the more optimization can be achieved compared to the classical link state protocol. [9],[10].

Each node in the network selects a subset (MPR set) from the nodes in its 1-hop symmetrical neighborhood to cover all 2-hop symmetrical nodes. In other words, each node in the strict 2-hop symmetrical neighborhood of N (set of neighbors of the node) must have a symmetrical link to the MPR (N). In addition, the MPR set should be as small as possible to reduce the overload of control traffic.

OLSR can also optimize reactivity to topological changes by reducing the interval time of the transmission for the periodic control message. OLSR is intended to operate in a fully decentralized manner without any central

entity. The protocol does not demand reliable transmission of control messages: each node regularly sends control messages and can suffer a reasonable failure some of them. These losses occur in wireless networks due to collisions or to other communication problems. [3]

In addition, OLSR does not require sequential message delivery. Each control message is associate with a sequence number that is incremented for each message. Thus, the receiver of a control message can simply identify the most recent information - even if the messages have been reorganized during transmission. Other pros for OLSR is supporting some protocol extensions such as sleep mode operation and multicast routing. These extensions can be introduced as additions to the protocol without breaking compatibility with older versions. OLSR does not need any changes to the format of IP packets. Thus, any existing IP stack can be deployed as it is: the protocol only interacts with the management of the routing tables. [3]

OLSR follows the logic of link state routing, which can be divided into two main branches. The first step is discovering the neighborhood by exchanging information about the link state of each node. The second step is the dissemination of the topology and the construction of the complete routing table for each node in the network. To provide the two main functions, OLSR broadcasts regularly and mainly two control messages to inform the situation of the topology: the HELLO message that is diffused by all the nodes to define one and two hop neighbors, detect the position of the location (symmetrical or asymmetrical) as well as the choice of MPRs. The Topology Control (TC) message is distributed only by MPR nodes and shows the list of neighbors that have selected this node as MPR. Both control messages are using to generate the routing tables.

The next section presents the most knowns attacks that affect OLSR routing protocol specially in its performance of routing.

3. MANET Routing Attacks

MANET is more vulnerable than the wired network due to mobility of nodes and the way used to exchange of data packets and control packets, generally, they passed from the source to the destination via different intermediate nodes [11] that can be malicious nodes inside the network. OLSR routing protocol can be affected by many active routing attacks which reduce its performances, in following we present three main routing attacks have negative impacts on OLSR protocol:

3.1 Black hole attack

The topology of the network in OLSR protocol was built by the information received from both OLSR control messages: HELLO and TC messages. The attacker starts the Black hole attack by sending incorrect information in its HELLO messages that broadcast to its 1-hop neighbors, these messages inform that malicious node has a direct link with several nodes that not really exist. The second step of the attacker is being an MPR node, due to the transparency in the algorithms of MPR selection calculated by each node. When a malicious node has been selected as an MPR node from its neighbors, it can receive all routing data and control packet, unfortunately, this attacker drops or stop forward them to the destination [12]. Figure 2 presents the mechanism used by the black hole attacker in OLSR protocol to affect its performances.

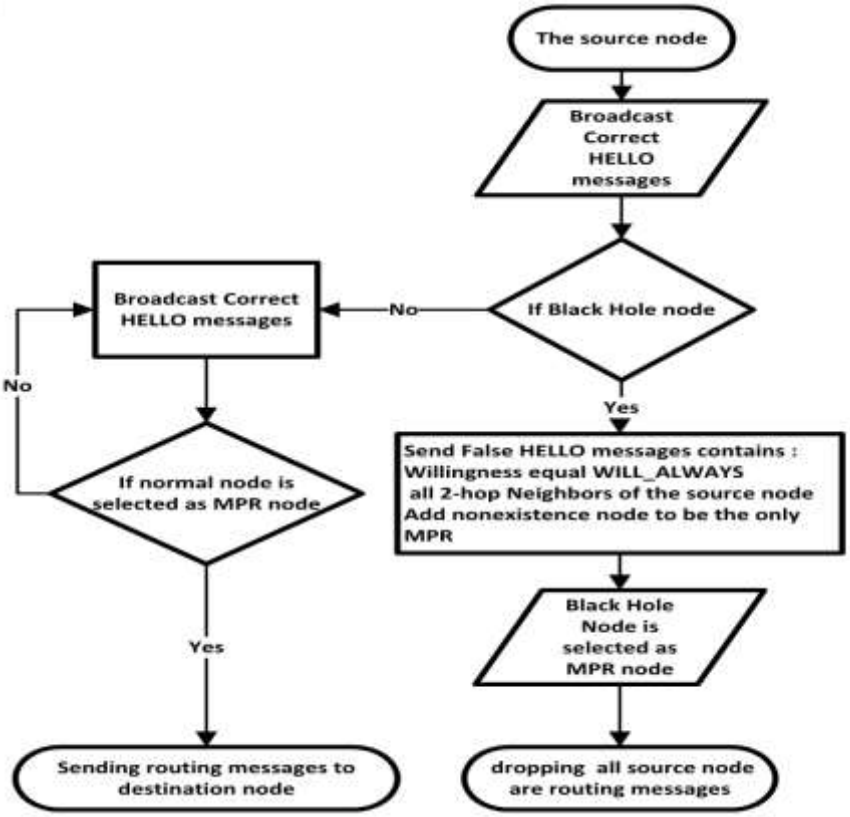

Fig. 2. The technic used by Black Hole attack in OLSR.

Black Hole attack in OLSR protocol can affect the neighbors of attacker when they select it as the only MPR node in their MPR set.

The second type of Black hole attack is the cooperative or multiple attack when two or more attackers collaborate between them by dropping or stop forwarding all routing messages received from these malicious nodes, each attacker send false HELLO message to its neighbors in order to be an MPR node, However the second attacker who ack as Black hole node and drop all received messages from the first attacker.

In our study we focus on the single Black hole attack that can implemented by each node in the network.

3.2 Node Isolation attack

Node Isolation Attack is a kind of service denial attack that concerns precisely OLSR protocol. Node Isolation Attack have main goal is shut off the communication of the target nodes with the other nodes which have a distance further than 2 hops away. The attacker in Node Isolation Attack do two technic for isolating any target node, the first way is deleting the IP address of the target nodes from 1-hop neighbor list that forwarded in HELLO message; in result, the neighbors that have 2-hop away from the target node cannot detect it present in the network [13]. The second technic for launching Node Isolation attack is done when the attacker becomes the only MPR for the target node, in this situation the malicious node stop generating and forwarding any TC messages for the target node and it will be isolated from the network. Figure 3 (a) and (b) demonstrate the effect of Node Isolation Attack.

Fig. 3. (a) Network topology received by smartphone H without attack.

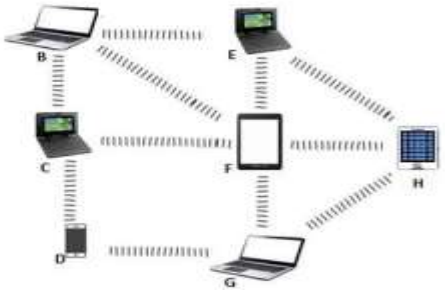

Fig. 3. (b) Network topology received by smartphone H with an attack.

In addition, when check the routing table of Smartphone H we remark the absence the destination entry of Smartphone A.

In the case of a node isolation attack, the attacker generally disconnects the target node from the network and makes it from being allowed to communicate with other neighbors [9]. The attacker can isolate the target node by deleting it IP address from HELLO message or hiding the victim node on the MPR selector set that send in TC messages.

3.3 Worm Hole Attack

In the Worm Hole attack, two attackers called by connivance nodes establish a virtual connection between them; the attack begins when the first attacker gets packets at one place in the network, and routes them through a tunnel to another location, and replay them from this point in the network. The virtual tunnel created between these colluding nodes is named as Wormhole Tunnel; however, in reality, these malicious nodes have distance longer than the normal wireless transmission range. The malicious nodes make the packets arrive in the Wormhole Tunnel with better metrics compared to normal multi-hop metrics [14]. With the use of a single long-range direction or a direct connection, the accomplice attacker creates the wormhole tunnel. Due to the broadcast nature of the wireless channel, it is also possible for a colluding attacker to create a wormhole path for packets not delivered to itself because it can hear and forwards them to the colluding attacker at the end of the wormhole. In the Wormhole attack, the position of the attacker must be very powerful relative to other nodes in the network to compromise the security of the network. Figure 4 presents an example of a Wormhole attack in MANET where nodes X and Y are the colluding nodes of the Wormhole Tunnel.

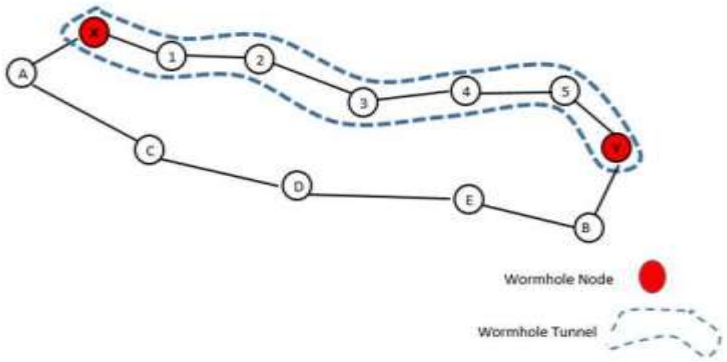

Fig. 4. Worm Hole attack in MANET.

In Worm hole attack, an attacker is listening secretly and behaves like a normal node, and at a certain point in time, it collects data and can leave the network. In most cases, all colluding nodes operate cooperatively and openly in a network [15].

The next section presents some previous work that develop MANET routing protocols to be more secure against these active routing attacks.

4. Related Work

The Black hole, the Worm hole and the Node Isolation attack are generally the most discussed attacks by researchers in wireless environments, and particularly in MANET environment. There are several methods that are designed to detect and mitigate the MANET routing attacks.

In the work [16] the authors presented four intrinsic properties of the OLSR protocol concerning control messages to be more secure against Node Isolation Attack, the first property is TC defined in the message TC must be

a subset of the HELLO message of the same source MANET node. The second property says that each node receives a TC message that presents itself as an MPR selector, the originator of the TC message must be near to this MANET node. The third property shows if a MANET node gets a TC message from its neighbors and notes that the TC message is presented as an MPR selector, this MANET node must have presented the sender of the TC message as MPR in its HELLO message first. Finally, the transmitter of the TC message must listen the same information as the TC messages which is transmitted by all its MPRs.

[9] suggest a fictitious node scheme for the detection as well as the prevention of certain network layer attacks such as the wormhole, the black hole as well as the gray hole attack, artificial nodes tend to operate at periodic intervals to verify the presence of any malicious node on the network. In same way, the authors examine the change in the number of fictitious nodes and the actual nodes in the network, this approach increases the surcharge of the network when there is a big number of nodes in the network.

The authors [17] proposed to use control message signatures to authenticate OLSR messages among network nodes. In this encryption system, a signature is provided by the originator of each OLSR control message and sends it together with a control message in the same message packet. The authors use the timestamp and match it to each signature to decide if the messages are recent or too old. This field avoids the duplication of messages previously transmitted and signed. When nodes have received a control message, it is required to check the timestamp and signature. If there are correct, the node addresses the message, otherwise it rejects the message and considers the original node as a malicious node. In this work, the authors define two methods of distributing the public key infrastructure (PKI), the first is proactive and aims to disseminate the public key to the nodes of the network, but the reactive method allows the nodes to request keys only when necessary.

The authors [18] proposed secure OLSR as a solution to prevent the standard OLSR routing protocol against network attacks such as wormhole attacks by protecting the discovery of neighbors, and the use of the wormhole

detection mechanism to defend themselves against this attack. This solution goes through three stages, on the one hand, by the detection of neighbors followed by the detection of wormholes and finally by the use of identity authentication, the authors present the theoretical analysis without any implementation, in addition, the proposed method uses additional messages for the exchange of identity authentication.

The authors [19] use the dummy node mechanism as a method where each node in the network checks whether a node isolation attack can be carried out through it. This technique prevents network nodes from sending false information about their neighbors and connectivity to other nodes by adding a fictitious node that does not exist in the network to avoid the attacker as the only MPR by applying the rules of contradiction designed to find an inconsistency between HELLO messages and the known topology.

In [20], the authors proposed a method allowing each node to check the accuracy of the HELLO message received from their neighbors at a hop before starting the MPR selection process. This method uses three extra control messages; to detect the malicious node, the three additional messages are the 2-hop request, the 2-hop response and NEQ (Node Exist Query). Each node uses these three additional messages to verify the presence of all the neighbors of the 2-hop node which are declared by their 1-hop neighbors; if a node is detected by the control messages, one or more nodes are not available by the other MPRs on the network, the authors prevent the node isolation attack.

the authors [21] proposed some modification in OLSR protocol, the first step star by using watchdog mechanism to monitor the neighbors, then they required authentication of the sender node by applying provable identity that calculates and update trust values of the corresponding nodes, finally, they add any mistrust node in a blacklist that regroups all nodes not able to be MPR. fuzzy Petri net (FPNT) is a proposed model suggested by [22], their mechanism evaluates trust values of mobile nodes by selecting a path with the maximum confidence value among all possible paths, an extended version of OLSR was developed using the proposed confidence model and the trust-based routing algorithm. [23] proposing a combined algorithm named by Jaya Cuckoo Search (JCS) algorithm, that

uses the Jaya algorithm and Cuckoo Search (CS) algorithm in order to initiate a secure route among the MANET nodes. They explain the of Jaya algorithm thanks to its powerful mechanism for optimization, whereas CS algorithm is a metaheuristic algorithm, whose goal is to speed up the rate of convergence with its single parameter value and is considered as a trouble-free optimization algorithm, this proposed technic is very complexed when there is a large number of nodes in MANET.

Other authors [24] have proposed a solution to detect the Black hole attack during communication in a VANET network, their method is based on a variable control chart in order to monitor the quality of a given process and to monitor in general the activities of network and finally they identify potential black hole attacks, the authors test the effeteness of their method by just one routing attack.

[25] propose trusted agent-based lightweight surprise check for malevolent node detection in MANET. This method divided in three phases, the first one is Lightweight surprise that check manager detects the malevolent node based on node forward rate and secure and location of the node. the second step named by cluster phase where the clusters are elected nodes based on the residual energy and utility of neighbors, and finally the phase of mobile agent that is used for data communication among cluster head to destination.

The work [26] introduces a new selection algorithm for all MPRs to avoid malicious neighbors and select the more secure route by adding a new criterion called degree of routing, the authors add new control message called by acknowledgment Hello Message to verify the information of HELLO message. The proposed method can detect and prevent only Black hole attack.

The next section we will present the main idea of our proposed method to detect any active routing attacks, by using the concept of Normality test and by applying the Shapiro Wilk method.

5. Proposed work

In our study, we present a new approach to detect any MANET routing attacks by applying the Normality Test that used in other different domains mainly in statistics, the goal of the normality test consists of deciding whether a dataset is well modeled by a normal distribution or not and calculating the probability that a random variable underlying the dataset is normally distributed. In MANET lot of research suggest adding or modifying the routing protocols either by including other control messages or by employing prevention methods for detecting the attack. Our approach for detection of the routing attacks suggests using the concept of Shapiro-Wilk [5] test in order to verify that the experimental distributions of the experiments are compatible with a particular theory distribution. Shapiro-Wilk test, it is very successful and efficient for lower numbers of the sample size s ($s \leq 50$) [27] . Some experts suggest the Shapiro-Wilk test as the best way to test the validity of the data. [28]. The benefits of our method are firstly we analyze just the results of the throughput metric in well-determined samples, also this method can detect any active routing attacks which stop or drop the routing packets and minimize the performance of through-put. In addition, our method does not request any modifications in protocol operation algorithms that means we save the same network overhead. The Shapiro-Wilk is based on the value of W which was determined as following:

$$W = \frac{\left[\sum_{i=1}^{\lfloor \frac{S}{2} \rfloor} a_i \left(x_{(s-i+1)} - x_{(i)}\right)\right]^2}{\sum_i (x_i - \bar{x})^2} \quad (1)$$

Where: $x_{(i)}$ is the sequence of sorted data and $[\frac{s}{2}]$ is the entire part of the ratio $\frac{s}{2}$, for $\bar{x}$ presents the average of the collection with:

$$\bar{x} = \frac{\sum x_i}{s} \quad (2)$$

a_i are constants obtained from the Shapiro-Wilk table [5] that contains all the values of a_i for the different sampling s.

The results of W can therefore be interpreted as the decision coefficient between the series of the sampling obtained from the normalization test named by W_Critical, and the actual empirical collection generated from the data. The values of W_Critical, which lists all the standard values with a varying risk α and effective are found in the table of Shapiro Wilk [5]. We reject the normality of W calculated when:

$$W_{Calculated} < W_{Critical} \quad (3)$$

Most active routing attacks in MANET have been affected especially the performance of throughput due to many lost and dropped packets in the network. For this reason, we choose to analyze the normality of the throughput measurement, which is defined as the total number of bites received successfully by the destination in a given time.

All in all, the calculated results W of the throughput for different samplings s have two meanings: in our case :

- If calculated W is bigger than $W_{Critical}$, he test of normality is approved and there are no active routing attacks.
- If calculated W is lower than $W_{Critical}$, the normality test is refused and we detect the existence of network attacks.

Our proposed method tests only if there is an active routing attack in the network with no action to eliminate it. The identification of active routing attacks in MANETs by the Shapiro-Wilk technique can be used as a simple way for any MANET routing protocol with no change in their algorithms in the same network overload.

6. Results and Analysis

This section evaluates the efficiency of our proposed method to detect the active routing attacks in MANET by using OLSR as routing protocol. In the first part we simulate 50 nodes under the effect of three routing attacks that vulnerable OLSR protocol these attacks are: Black hole, Worm hole and Node Isolation attacks. The implementation was realized by the Simulator Network (NS-3). ns-3 is a discrete-event network simulator for Internet systems, designed primarily to use in research and education. ns-3 is open-source software, licensed under GNU GPLv2, and is accessible to the public for research, development and deployment [29].

6.1 Simulation and results

To implement the normality test in MANET to detect the routing attacks , we simulated 50 nodes under Black Hole and Worm Hole attack in Random Waypoint Mobility Model [30], and due to the technic use by Node Isolation Attack we simulate it in Constant Waypoint Mobility Model . Table 1 details all other variables that are used in the simulation.

Table 1. Parameters of Simulation in NS3.

N°	Parameter	Value
1	Server Simulator	Dell Intel Xeon ®
2	Simulator Version	NS3 (3.26)
3	Number of Nodes	50
4	Time of Simulation	50
6	Model of Mobility	Random and Constant Waypoint mobility model
8	Rate of Data	2 Mbps
10	Size of Packet Sent	64 Bytes
11	Protocols Evaluated	OLSR
13	Routing Attacks	Black Hole attack, Worm Hole attack and Node Isolation Attack
14	Node Speed	5 m/s
15	Pause Time	0 second
16	Network area	1000x1000 m
17	The metric	Throughput

Figure 5 illustrates the results achieved for Shapiro Wilk (W) values under two situations with and without Black hole attack.

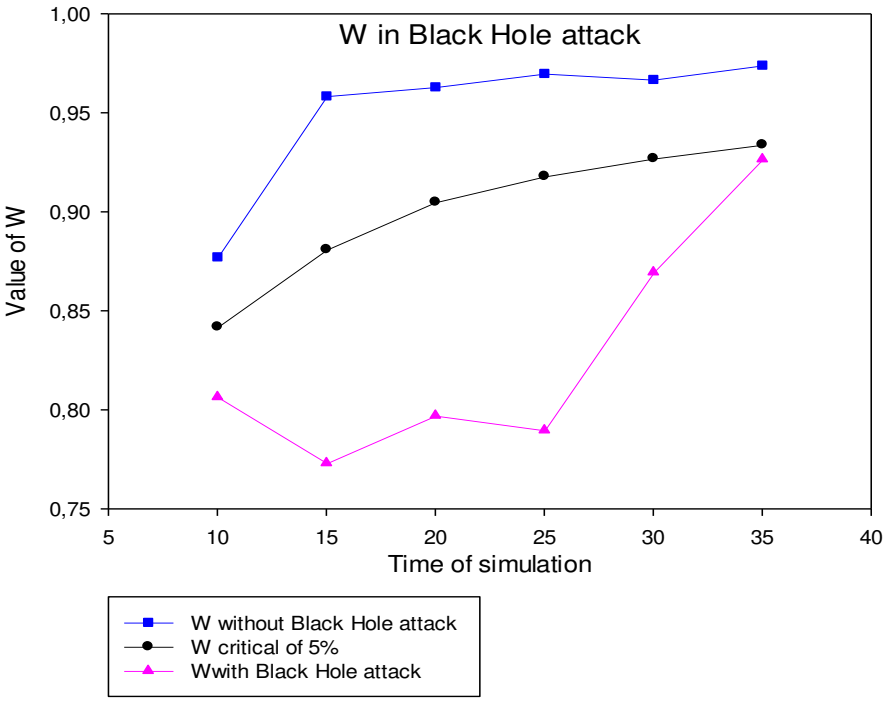

Fig. 5. W of Throughput with and without Black Hole Attack.

In MANET without attack we show that the values of W have higher values compared to the Critical W in different times of the simulation; these values start by W equal 0.87 and become increasing during the simulation. We can explain these values by the nature of OLSR routing protocol that need some time to build the view and topology of network by the information received from HELLO and TC messages, in standard OLSR version the interval time of HELLO message is 2 seconds. However, TC interval time is 5 seconds. In addition, all W values without Black hole attack confirm the normality assumption thanks to higher W calculated of throughput. On the other hand, when the Black Hole attack was launched in the network, the W of throughput calculated have fewer values than the Critical W for different sampling. These W values with Black Hole attack approve the not normality of the network

due to negative effect of Black Hole attack which drops the routing packets forwarded by the attacker, the consequence is minimizing the throughput of the network. Our method can detect the black Hole attack in fast way without any modification in the OLSR protocol and without any additional device.

Figure 6 present the results of W with and without Node Isolation attack, we remind that the mobility model used for this attack is the Constant Waypoint Mobility Model (CWPM), we explain that by the nature of attack which demanded a lower or fixed mobility to isolate the target node which must be within the same range of the attacker.

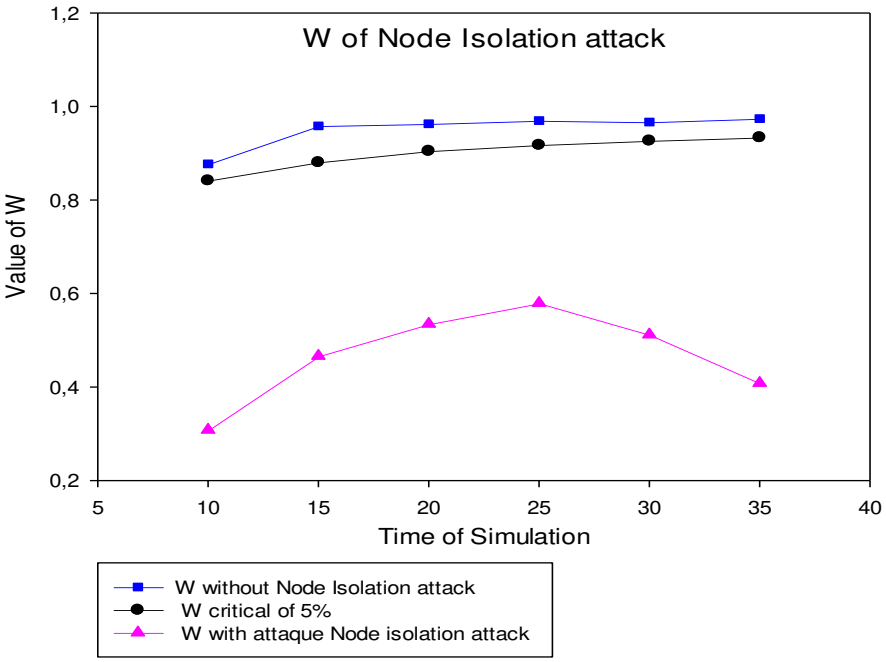

Fig. 6. W of Throughput with and without Node Isolation Attack.

From figure 6 we show that W calculated in a normal situation without any Node Isolation Attack gives higher values compared to critical values of W in a normal situation, in the first 10 seconds we remark that the value of Shapiro Wilk is more than 0.8 and increases on an ongoing basis, the meaning is OLSR protocol has performance

throughput thank to normal control messages send and received by each node in the network. However, when Node Isolation attack is available, the value W decreases during all periods of simulation. The lower value is less than 0.3 in the first 10 seconds of simulation and the higher value is found under the 25 seconds, all Shapiro Wilk values confirm that the negative effect of Node Isolation attack is more remarkable due to lower W rate during all simulation time compared to the normal or critical W. The Constant Waypoint Mobility Model applied in this attack considers as an addition factor to increase the effect of Node Isolation Attack compared to both other attacks which simulated in Random Waypoint Mobility Model. The Shapiro-Wilk method detect Node Isolation Attack in efficient manner during all simulation time.

The results of figure 7 present the values calculated of Shapiro Wilk with and Without Worm hole Attack. We are modifying the OLSR protocol to create a virtual tunnel between two far away nodes. The mobility model applied for simulate the Worm hole attack is Random Waypoint Mobility Model (RWPM).

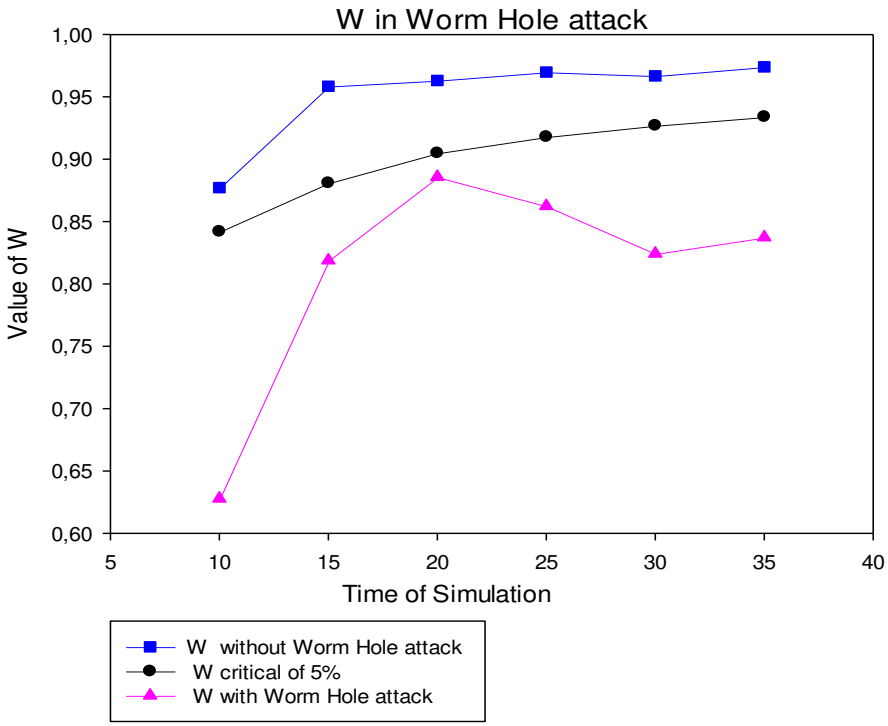

Fig. 7. W of Throughput with and Worm Hole attack.

Figure 7 indicates that the results achieved from the calculate of W without Worm hole attack is similar to W simulated in Figure 5, when there is no Black Hole attack due to the same environment of simulation used in both attacks; in addition W without Worm hole attack has superior values than the Critical W, and by applying the signification of Shapiro-Wilk we infer more credible the compatibility of throughput with the Normality Test. Moreover, when the Worm Hole attack was launched in the network, we remark that W has been decreasing during all first 35 seconds, in this case, we reject the hypothesis of the normality and by the end, the detection of Worm Hole attack have been done in simple and efficient may.

The results of Shapiro Wilk for the throughput in MANET that affect by Black hole, Worm hole or Node Isolation attacks confirm their present in the network and by the end the detection of them without any modification on the protocol.

In the sext part of testing, we create a real MANET with wireless devices Which configure to use standard version of OLSR in their communication.

6.2 Case study

To test the effeteness of our proposed method for detecting the routing attacks in MANET. We create small ad hoc network by using six wireless devices that composed three personnel computers and three smartphones. All These MANET devices are connected by wireless channel without any access point. Figure 8 shows the topology created in real environment. In addition, we configure all nodes with OLSR routing protocol to ensure the connectivity between them. The routing attack chosen in this analysis is Node Isolation Attack that can launched in small density contrary to Black hole and Worm hole which required more other devices to affect the network.

Fig. 8. Topology of MANET in real environment

Due to nature of Node Isolation attack that become More vulnerable in lower or fixed Mobility of nodes in MANET, we fixed all devices in their positions without any movement and we select the white PC as attacker because we have the possibility to change OLSR in its algorithm to isolate the target node, in our case is the circler smartphone, this latter has one MPR in it routing table which is the attacker.

Two scenarios are simulated in this real case study, the first one test the performance of ping command without attack where the destination node is the target smartphone. In the next step we calculate the throughput of the network reckons on the results of ping command then we choose the first 35 samples for checking the Shapiro Wilk test.

In the second scenario we save the same topology and configuration but we integer the Node Isolation attack in white PC to isolate the target smartphone; after that we test the connectivity to reach the victim node with ping command. Figure 9 and 10 present the results of Shapiro Wilk test for 35 samples of throughput with and without Node Isolation attack.

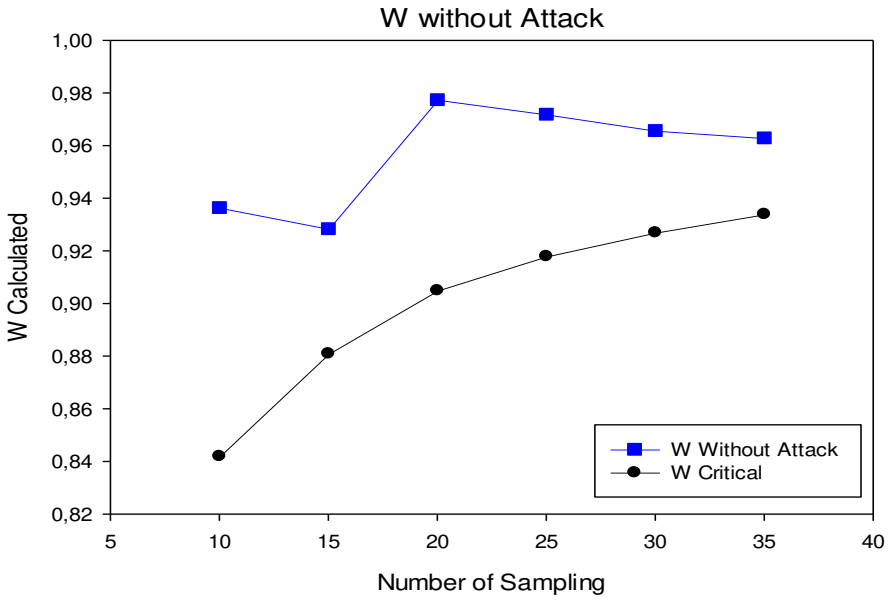

Fig. 9. W calculated of throughput in real environment without attack.

To calculate the values of W we are starting by the first 10 responds of ping command and each respond have different throughput due to time taken in the request and the reply to reach the destination (in our situation is the target node). And by applying the Eq. (1) of Shapiro-wilk we can show that W of 10 samples have higher value than the critical W, this result is decreased in the 15 sampling, however it becomes increasing during all other different samples of throughput. To test the normality of our network we apply the rule of Eq. (3), we conclude the absence of any active routing attack that reduce the performance of throughput in MANET.

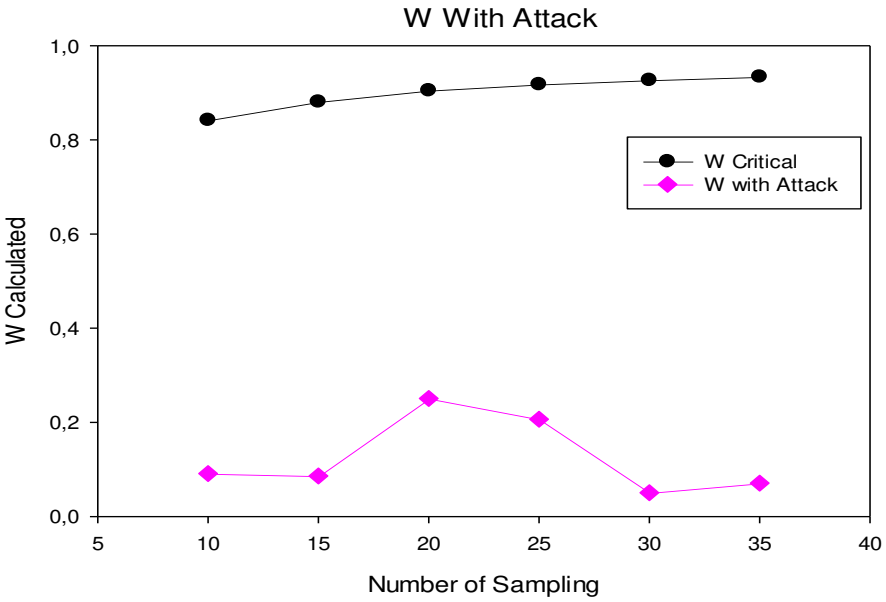

Fig. 10. W calculated of throughput in real environment with attack.

For the second scenario the OLSR routing protocol have been modified in the attacker device to isolate the target smartphone, this attack is done by sending false HELLO messages that remove the IP address of the victim, these messages are generated by the attacker and forwarded to its neighbors. When we check the routing table of other devices, we remark the absence of any entry for the target node, by the end it become isolated from the network.

The W calculated for the 10 first samples of throughput has less value compared to the critical W referenced in the Shapiro Wilk table [5]. The same result is shown in 15 samples, in the other hand the W calculated becomes increasing in the 20 and 25 samples but its have values less than 0.3, after that we show a reduce value for 30 and 35 samples, and by applying the hypothesis of normality test in Shapiro Wilk, we detect the presence of active routing attack that affect the throughput of MANET, in this experience is the Node Isolation attack

6.3 Comparative study between existing solutions

This part of section presents a comparative analysis of previous solutions that detect some active routing attacks. Table 2 compares the different solutions with their strategies used for the detection in OLSR routing protocol.

Table 2. Comparative study of network threat detection solutions using the OLSR protocol.

Solution	Detection of Worm hole attack	Detection of Black hole attack	Detection of Node Isolation Attack	New Control messages added	Network Overhead	Proposed solution base
[16]	No	No	Yes	No	Yes	IDS System
[17]	Yes	Yes	Yes	Yes	Yes	Modification in OLSR + Identification System
[18]	Yes	Yes	No	Yes	Yes	New control Messages Added + Authentication
[20]	No	No	Yes	Yes	Yes	New control messages + Modification of the MPR algorithm
[22]	Yes	No	No	Yes	Yes	fuzzy Petri net (FPNT) algorithm
[19]	No	No	Yes	Yes	Yes	Using of Fictitious Nodes
[25]	Yes	Yes	No	No	Yes	lightweight surprise check scheme

[9]	Yes	Yes	No	Yes	Yes	Modification in Control Messages
[23]	Yes	No	No	Yes	Yes	Jaya Cuckoo Search (JCS) algorithm
[21]	Yes	Yes	No	Yes	Yes	Trust Node Mechanism
[24]	Yes	No	No	No	No	Mechanism of variable control chart
[26]	No	Yes	No	Yes	Yes	New MPR Computation
Our proposed detection method	Yes	Yes	Yes	No	No	The law of Normality

Based on our analysis of previous work on detecting network attacks that affect the performance of the OLSR protocol, they are divided into three categories: those that modify the protocol version by adding new control messages, which presents an additional overhead in traffic on a shared channel, in other words, the increase in messages in the MANET network can cause congestion and consequently the OLSR protocol loses more packets and the end-to-end time will be extended. The second category of solutions offers cryptography mechanisms for authentication and identification of network nodes or encryption of OLSR messages, these mechanisms require encryption and cryptography algorithms or certificates. Therefore, we can say that methods based on cryptography are a bit ahead of those who do not use it. Some solutions use additional algorithms, or an IDS system or equipment in order to detect network threats.

Our approach does not require any additional hardware, it processes data exchanged between network nodes in order to detect network attacks. On this basis, we say that our approach analyzes the minimum amount of information to detect threats. There is also the evolutionary side of the approach, as described in the results section, three

scenarios of three network attacks using different mechanisms are studied. We were able to detect these attacks while still keeping the standard version of the OLSR protocol.

7. conclusion

In this work we are presenting a new efficient method to detect any active routing attacks that affect the throughput of OLSR routing protocol by applying the concept of Normality Test and using Shapiro-Wilk formula. To test the effeteness of our proposed method, three popular active routing attacks that affect the throughput of OLSR protocol were implemented in NS3 simulator. The results obtained for W of throughput under the Black hole attack, Worm Hole attack and Node Isolation Attack confirm the reject of normality hypothesis. By the end, we detect the present of active routing attacks in the network, in the other side when the OLSR operates in normal condition without any routing attacks, we found higher values of W calculated compared to critical W posed by Shapiro-Wilk to accept the Normality Test and we confirm the absence of any active routing attacks. Our next work will be applied our proposed method in real environment by creating Ad hoc network and integer all routing attacks to test the detection in real time.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] S. Gurung et S. Chauhan, « A novel approach for mitigating gray hole attack in MANET », *Wirel. Netw.*, vol. 24, nº 2, p. 565-579, févr. 2018.
[2] M. S. Raheel, S. Iranmanesh, et R. Raad, « A novel Energy-Efficient Video Streaming method for decentralized Mobile Ad-hoc Networks », *Pervasive Mob. Comput.*, vol. 40, p. 301-323, sept. 2017, doi: 10.1016/j.pmcj.2017.07.008.
[3] T. Clausen et P. Jacquet, « Optimized Link State Routing Protocol (OLSR) », janv. 03, 2003.
[4] R. Kumar, S. Lokesh, et Ramya Devi, « Identifying Camouflaging Adversary in MANET Using Cognitive Agents », *Wirel. Pers. Commun.*, vol. 102, nº 4, p. 3427-3441, févr. 2018.
[5] S. S. Shapiro et M. B. Wilk, « An Analysis of Variance Test for Normality (Complete Samples) », *Biometrika*, vol. 52, nº 3/4, p. 591-611, 1965, doi: 10.2307/2333709.
[6] D. Park, S. Park, W. Kim, I. Rhiu, et M. H. Yun, « A comparative study on subjective feeling of engine acceleration sound by automobile types », *Int. J. Ind. Ergon.*, vol. 74, p. 102843, nov. 2019, doi: 10.1016/j.ergon.2019.102843.
[7] A. Boushaba, A. Benabbou, R. Benabbou, A. Zahi, et M. Oumsis, « Multi-point relay selection strategies to reduce topology control traffic for OLSR protocol in MANETs », *J. Netw. Comput. Appl.*, vol. 53, p. 91-102, juill. 2015, doi: 10.1016/j.jnca.2015.03.008.
[8] D. Zhang, T. Zhang, Y. Dong, X. Liu, Y. Cui, et D. Zhao, « Novel optimized link state routing protocol based on quantum genetic strategy for mobile learning », *J. Netw. Comput. Appl.*, vol. 122, p. 37-49, nov. 2018, doi: 10.1016/j.jnca.2018.07.018.
[9] R. Bhuvaneswari et R. Ramachandran, « Denial of service attack solution in OLSR based manet by varying number of fictitious nodes », *Clust. Comput.*, vol. 22, nº 5, p. 12689-12699, sept. 2019, doi: 10.1007/s10586-018-1723-0.
[10] J. Toutouh, S. Nesmachnow, et E. Alba, « Fast energy-aware OLSR routing in VANETs by means of a parallel evolutionary algorithm », *Clust. Comput.*, vol. 16, nº 3, p. 435-450, sept. 2013, doi: 10.1007/s10586-012-0208-9.
[11] Vinay Singh, Ajit Singh, et Malik Mubasher Hassan, « Survey: Black Hole Attack Detection in MANET », *Proceedings of 2nd International Conference on Advanced Computing and Software Engineering (ICACSE) 2019*, avr. 2019.
[12] A. Nabou, M. D. Laanaoui, et M. Ouzzif, « Evaluation of MANET Routing Protocols under Black Hole Attack Using AODV and OLSR in NS3 », in *2018 6th International Conference on Wireless Networks and Mobile Communications (WINCOM)*, oct. 2018, p. 1-6, doi: 10.1109/WINCOM.2018.8629603.
[13] B. Kannhavong, H. Nakayama, N. Kato, Y. Nemoto, et A. Jamalipour, « Analysis of the node isolation attack against OLSR-based mobile ad hoc networks », in *2006 International Symposium on Computer Networks*, juin 2006, p. 30-35, doi: 10.1109/ISCN.2006.1662504.
[14] Yih-Chun Hu, A. Perrig, et D. B. Johnson, « Wormhole attacks in wireless networks », *IEEE J. Sel. Areas Commun.*, vol. 24, nº 2, p. 370-380, févr. 2006, doi: 10.1109/JSAC.2005.861394.
[15] G. Farjamnia, Y. Gasimov, et C. Kazimov, « Review of the Techniques Against the Wormhole Attacks on Wireless Sensor Networks », *Wirel. Pers. Commun.*, vol. 105, nº 4, p. 1561-1584, avr. 2019, doi: 10.1007/s11277-019-06160-0.
[16] M. Wang, L. Lamont, P. Mason, et M. Gorlatova, « An effective intrusion detection approach for OLSR MANET protocol », in *1st IEEE ICNP Workshop on Secure Network Protocols, 2005. (NPSec).*, nov. 2005, p. 55-60, doi: 10.1109/NPSEC.2005.1532054.

[17] Cedric Adjih, Thomas Clausen, Philippe Jacquet, Anis Laouiti, Paul Muhlethaler, et Daniele Raffo, « Securing the OLSR protocol ». Théme COM-Systémes communicants projet HIPERCOM, févr. 2005.
[18] Fan Hong, Liang Hong, et Cai Fu, « Secure OLSR », *Proceedings of the 19th International Conference on Advanced Information Networking and Applications*, 2005.
[19] Nadav Schweitzer, Ariel Stulman, Asaf Shabtai, et Roy David Margalit, « Mitigating Denial of Service Attacks in OLSR Protocol Using Fictitious Nodes », *IEEE Trans. Mob. Comput.*, vol. 15, nº 1, p. 163-172, janv. 2016.
[20] Mohanapriya Marimuthu et Ilango Krishnamurthi, « Enhanced OLSR for Defense against DOS Attack in Ad Hoc Networks », *J. Commun. Netw.*, vol. 15, nº 1, févr. 2013.
[21] A. N. Dehkordi et F. Adibnia, « Securing the OLSR Routing Protocol », vol. 2, nº 1, p. 10, 2020.
[22] S. Tan, X. Li, et Q. Dong, « Trust based routing mechanism for securing OSLR-based MANET », *Ad Hoc Netw.*, vol. 30, p. 84-98, juill. 2015, doi: 10.1016/j.adhoc.2015.03.004.
[23] Ch. Ram Mohan et V. R. Ananthula, « Reputation-based secure routing protocol in mobile ad-hoc network using Jaya Cuckoo optimization », *Int. J. Model. Simul. Sci. Comput.*, vol. 10, nº 03, p. 1950014, mai 2019, doi: 10.1142/S1793962319500144.
[24] B. Cherkaoui, A. Beni-hssane, et M. Erritali, « Variable control chart for detecting black hole attack in vehicular ad-hoc networks », *J. Ambient Intell. Humaniz. Comput.*, mars 2020, doi: 10.1007/s12652-020-01825-2.
[25] A. Aranganathan et C. D. Suriyakala, « An efficient secure detection and prevention of malevolent nodes with lightweight surprise check scheme using trusted mobile agents in mobile ad-hoc networks », *J. Ambient Intell. Humaniz. Comput.*, vol. 10, nº 9, p. 3493-3503, sept. 2019, doi: 10.1007/s12652-018-1069-8.
[26] A. Nabou, M. D. Laanaoui, et M. Ouzzif, « New MPR Computation for Securing OLSR Routing Protocol Against Single Black Hole Attack », *Wirel. Pers. Commun.*, nov. 2020, doi: 10.1007/s11277-020-07881-3.
[27] N. M. Razali et Y. B. Wah, « Power Comparisons of Shapiro-Wilk, Kolmogorov-Smirnov, Lilliefors and Anderson-Darling Tests », *J. Stat. Model. Anal.*, vol. 2, nº 1, p. 21-33, 2011.
[28] H. C. Thode, « Normality Tests », in *International Encyclopedia of Statistical Science*, M. Lovric, Éd. Berlin, Heidelberg: Springer, 2011, p. 999-1000.
[29] « NS3 Homepage ».
[30] E. Hyytiä et J. Virtamo, « Random waypoint mobility model in cellular networks », *Wirel. Netw.*, vol. 13, nº 2, p. 177-188, avr. 2007, doi: 10.1007/s11276-006-4600-3.

Figures

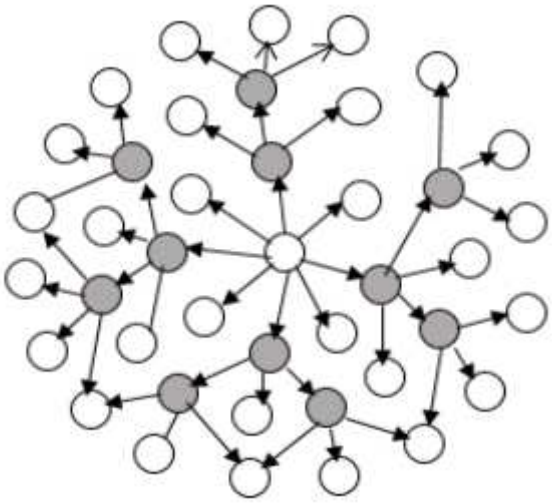

Figure 1

Flooding by the technic of MPRs in OLSR4

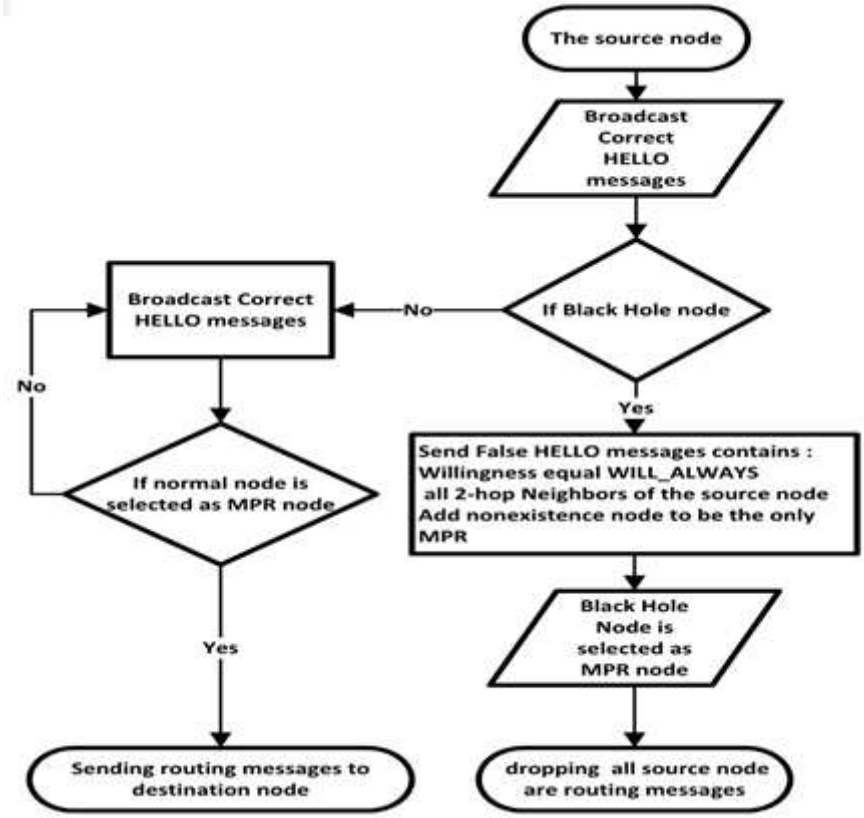

Figure 2

The technic used by Black Hole attack in OLSR.

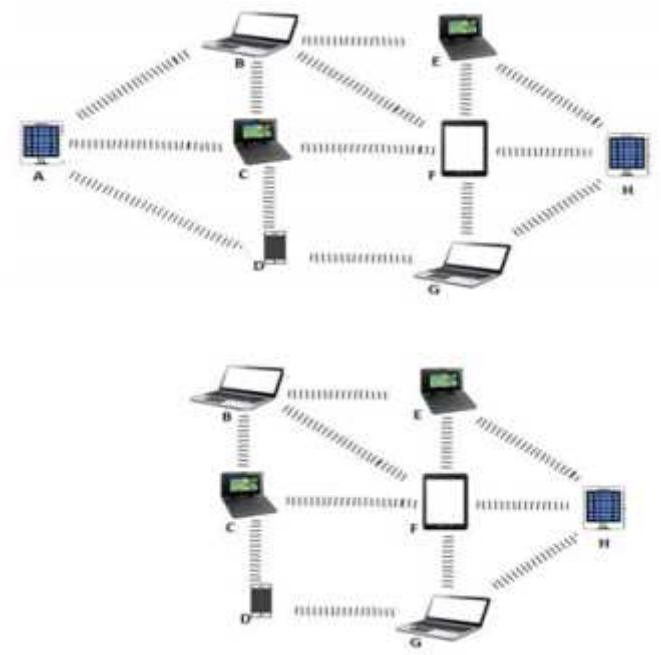

Figure 3

(a) Network topology received by smartphone H without attack. (b) Network topology received by smartphone H with an attack.

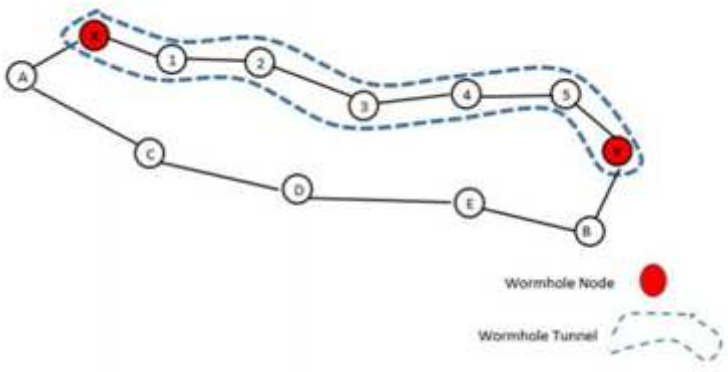

Figure 4

Worm Hole attack in MANET.

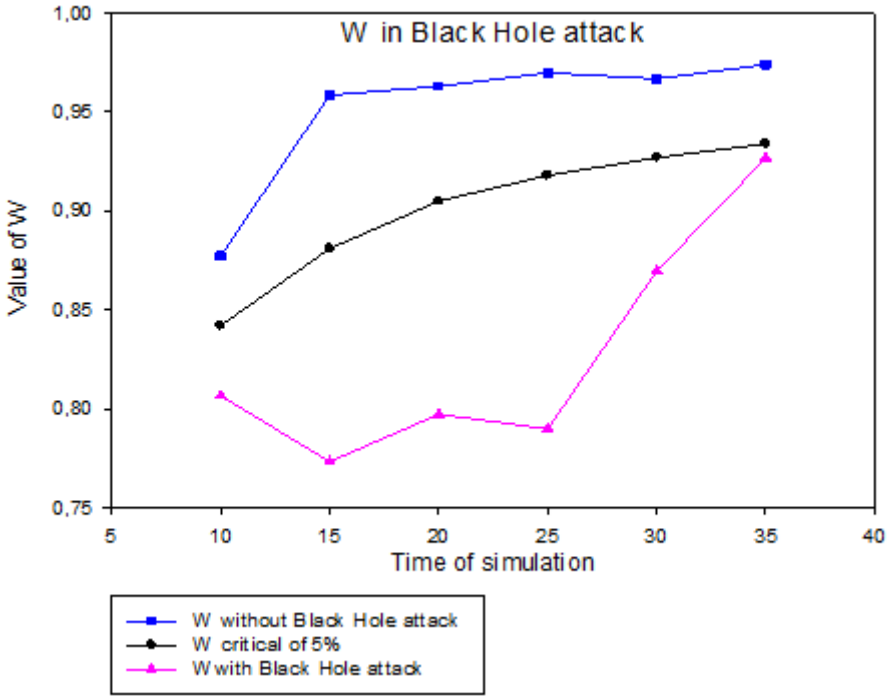

Figure 5

W of Throughput with and without Black Hole Attack.

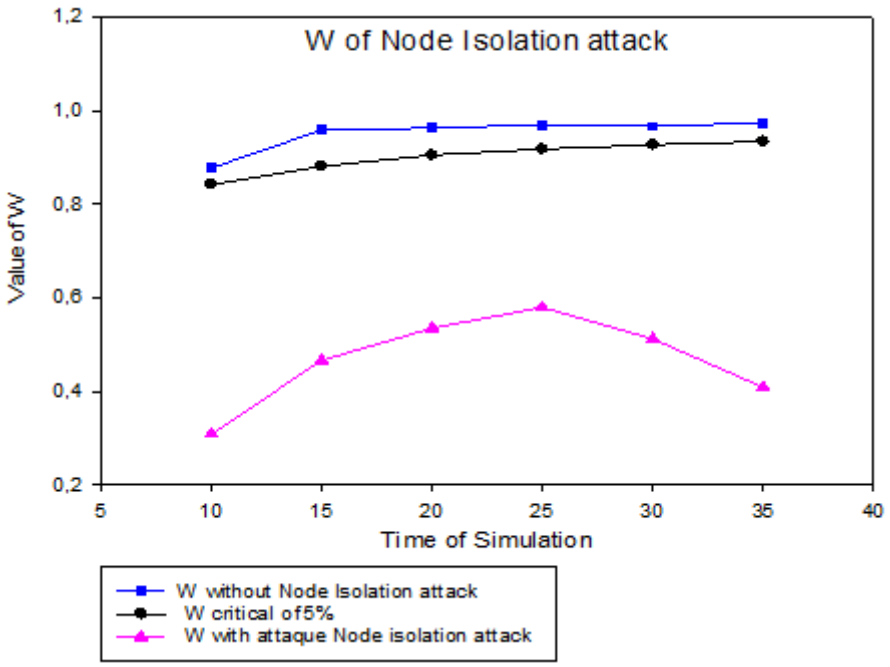

Figure 6

W of Throughput with and without Node Isolation Attack.

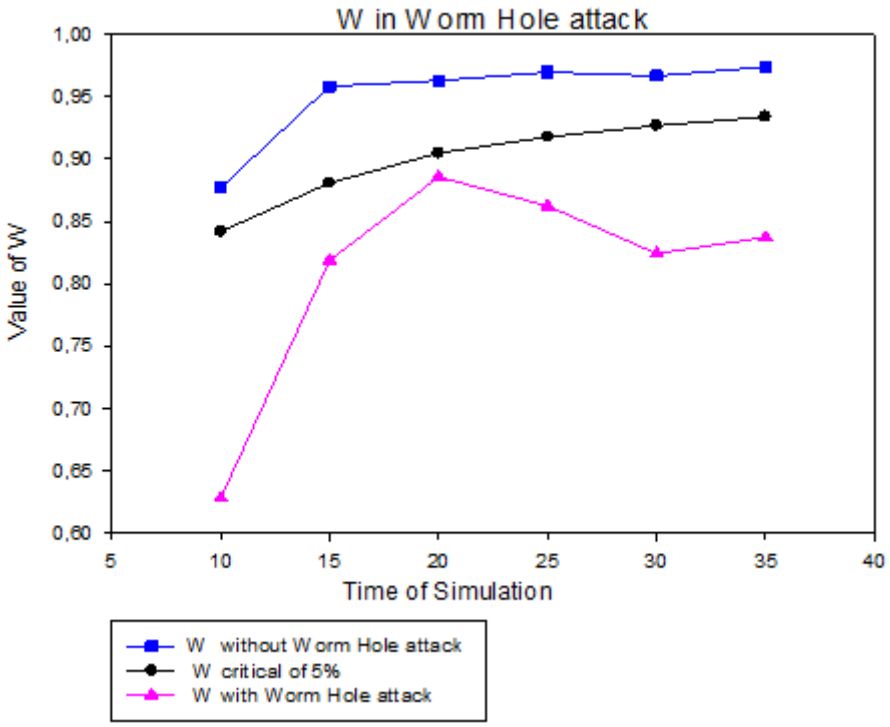

Figure 7

W of Throughput with and Worm Hole attack.

Figure 8

Topology of MANET in real environment

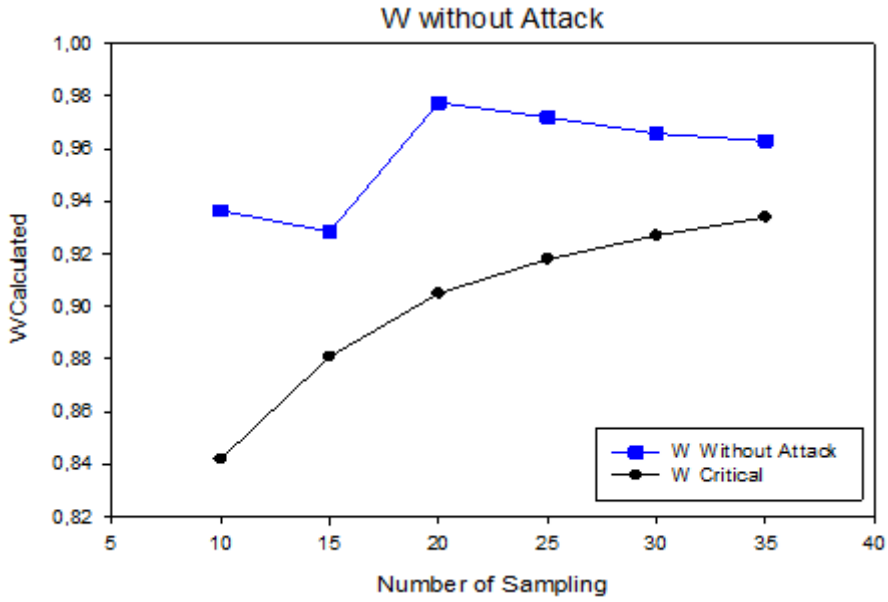

Figure 9

W calculated of throughput in real environment without attack.

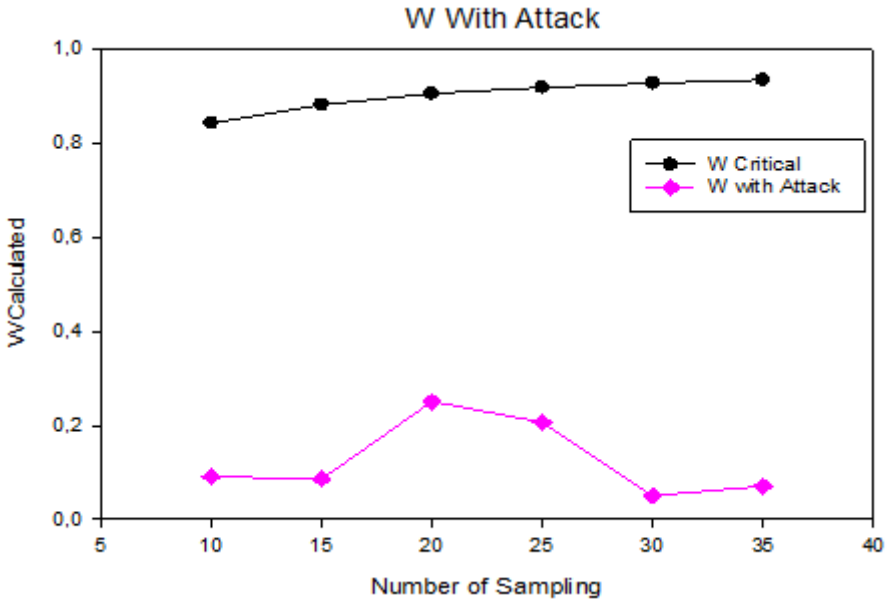

Figure 10

W calculated of throughput in real environment with attack.