An Effective Method of Security Against Wormhole Attack

Mohamed Amine Ferrag and Mehdi Nafaa

***Abstract*—A major problem facing researchers today in the field of ad hoc networks is safety and preservation of the integrity of such networks. Among the many attacks recorded in the literature, wormhole attack remains a severe attack and not completely solved, particularly in ad hoc network configuration where OLSR is used as routing protocol. We have chosen the OLSR routing protocol because it is the most widely used ad hoc community. In general the attacker can delete, modify, copy control messages to send false messages. Our scheme consists of detecting the type of attack, the checks and then ends with alert the nodes of mobile social network. These three elements is based on the addition of five messages " Hreq , Hrep, HAlert, Probing and ACKprob" in the OLSR protocol. For the exchange of a package of Hreq , Hrep and HAlert ; and to provide authentication as well confidentiality. We have proposed the dual use of public key encryption; the message will be decrypted only by the true recipient and to ensure safe exchange of a package of Probing and ACKprob, we proposed an architecture through the use of RSA and MD5 to sign messages. The proposed solution is easy to deploy and requires no time synchronization or location information nor does it require any special equipment or complex calculation. The performances of this approach show a high detection rate under various scenarios.**

***Index Terms*—Wireless ad hoc networks, routing protocols, olsr, security, wormhole attack, MD5, RSA.**

I. Introduction

Wireless networks are inherently more sensitive to security issues. For ad hoc networks, the main problem does not lie in both the physical media but mainly in the fact that all nodes are equivalent and potentially necessary to operate the network. In an ad hoc network attacks can be directed against a service station or those of the network. The main consequences of these attacks, presented in [1], are summarized below:

- The introduction of a routing loop.
- The creation of a black hole that is to redirect traffic to a node that does not retransmit the information.
- The division of network into multiple subnets to block trade between nodes belonging to different subnets.
- No retransmission of messages to node.
- The stop of a node due to its lack of energy.

Manuscript received February 16, 2012; revised April 20, 2012.

M. A. Ferrag is PhD student in networks and computer security at University Badji Mokhtar, ANNABA, and Algeria (e-mail: mohamed.amine.ferrag@gmail.com).

M. Nafaa is currently teaches in the Departement of Computer Science University Badji Mokhtar, Annaba, Algeria (e-mail:mehdi.nafaa@gmail.com).

II. The Attacks on the OLSR

The routing protocols operate in two distinct phases: a phase for discovery of network topology in which information control on the network topology knowledge is exchanged, and then a phase of transmission of data messages in which data is sent from a source to a destination. Unlike wired where routing operations are generally conducted by the physical interconnection dedicated and administered by a government legitimate, in mobile ad hoc these operations are entirely the responsibilities of the nodes that comprise them. This operating characteristic raises many security issues. In looking at the routing protocol OLSR, It is expected that each node generates messages properly control HELLO and TC and maintain a view of the network topology derived from the messages it receives. But as the nodes are autonomous, deviant behavior rules defined by the protocol may occur and cause deformations on the order of the topology network built.Table1 is a list of possible attacks on the protocol operations and undistorted messages (such as replay or non-broadcast control messages), then a list of attacks by construction or alteration of control messages.

III. Related Work

All methods for securing routing protocols based on cryptographic methods offer security guarantees in terms of confidentiality, authentication and message integrity; they are not resulting in such attacks. This attack affects particularly the protocols based on a neighborhood discovery phase direct exchange of control messages for roles and paths between nodes. It can lead to conflicts in relationships established neighborhood. The resources currently available in the literature are:

- Cons-measurement at the physical layer;
- Specific material module and time window ;
- Clock synchronization loose and geographic positioning of the nodes;
- Clock synchronization and fine time window;
- Directional antennas.

A. Cons Measurement at the Physical Layer

The first work addressing the attack of the wormhole based on material and techniques of signal processing. It is suggested that a secret method of modulating bit radio signal. The signal can be demodulated only by authorized nodes.

A vulnerability of this method is that the method is not stored in a space of trust, which can lead to unauthorized opponents to compromise legitimate node in the network to obtain the necessary access or opponents allowed to disclose their knowledge of the method. (It might be considered complementary mechanisms for securing code modulation /

demodulation as obfuscation, or the star of an environment resistant to weathering).

In security terms, this method allows only a defense against the attack of the wormhole nodes opponents led by external (unauthorized) to the network, that is to say nodes that do not have the key cryptography. It also raises the question of establishing / negotiating the secret method between legitimate nodes in the network [2].

B. Clock synchronization and Time Window: Packet leashes

Packet leashes is a solution for detecting the attack wormhole proposed by Hu [3].

A leash is the information (time or geographical location)that is included in each of the packets on the network and serves to restrict their maximum distance transmission. Two methods of using leashes are presented:

- A first based on the support of a geographic positioning service.
- The second is based on an accurate clock synchronization between nodes.

*Geographical Leashes***.** The geographical leashes to ensure the distance between the receiver and sender of a message. The mechanism requires that each node knows its own geographic position, and secondly that the clocks of all nodes are loosely synchronized (on the order of a millisecond).During transmission of a message, the sending node includes in the message an authentic version of his own location and time of issue. A receiving node uses the information leashes encapsulated in the received message and its own geographical position and time of receipt of the message recorded to estimate an upper bound of the distance from the transmitter. Taking into considerations some variables such as maximum velocity nodes, the maximum error in the system clock synchronization, and the maximum possible error in the system of geographical passionately, the upper bound of the distance between the transmitter and the receiver can then be determined. If the calculated distance is greater than the maximum range of transmission, then the link probably wrong. One limitation of this method is that it relies on a positioning system. In fact, GPS technology is currently inoperative in the enclosed spaces (such as buildings), underwater environments, environments subject to strong magnetic radiation, etc. It also raises the question of state of location information provided by GPS technology. The authors state that according to the state of the art in GPS technology, it is possible to achieve an accuracy of about 3m.

*Temporal leashes***.** The temporal leashes ensure that each message sent through the network until the expiration time is not exceeded, and then the packet is rejected. A non-negligible prerequisites of the method is an accurate clock synchronization between all nodes in the network. Under this method, an issuer includes in each message an authentic version of the issue time. In the verification phase, a receiver compares this value to the time of receipt of the message. In a variant of temporal leashes, a transmitter determines the expiration time at which a message should be accepted and included this information in the leash. In summary, the method rests on the travel time of a message and then the speed of light to determine its approximate distance travel. An implicit assumption is that time of message processing, transmission and reception is negligible.

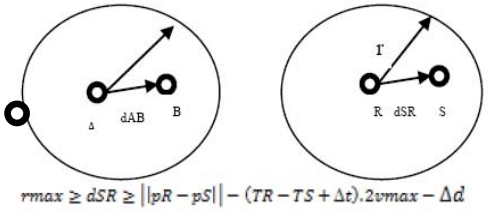
Discussion. Both the approach based on temporal leashes and the one based on the geographical leashes require the addition of authentication data for each message in order to protect leashes (against identity theft and modification).Authentication introduced a surcharge in terms of treatment and time (because of ground operations, audits and signing inbound and outbound).While the authors discuss mechanisms to improve the operational efficiency of signature, it is clear that the delays associated with them may make potentially terminal imprecise and unreliable. An overcost in terms of communication is mainly due to the addition of an authentication protocol with distribution / key exchange. Finally, a large storage capacity for authentication scheme based on a chopped tree is required.

TABLE I: SUMMARY OF ATTACKS ON THE OLSR

			Conflict roads	Loss Connectivity	Loss message	target
Traffic Generation incorrect	HELLO	Usurpation identity	X	X	X	All nodes
		Usurpation Link	X	X		Knots in the direct vicinity of the opponent
	TC	Usurpation identity	X	X	X	All nodes
		Usurpation Link	X	X		Subset Node
	Attack ANSN			X	X	
Relay Traffic incorrect	Changing message		X	X		
	Black hole			X	X	Node specific
	Replay		X	X	X	
	Wormhole			X		Subset of nodes close to the hole
	MPR					Node specific

C. Geographical Positioning

Directional antennas**.** Nodes equipped with directional antennas using sectors (a total of 8, namely N, S, E, W, NE, NW, SE, SW) to communicate between them. A node that receives a message from a neighbor gets a rough information (N, S, E, W) on its position. He knows the relative orientation of its neighbor over himself. These are additional bits of information (angle of arrival of the signal) that are exploited in some way to facilitate the detection / discovery of wormhole attacks. In [4], Hu and Evans proposed a method for checking the neighborhood using directional antennas. The neighboring nodes examine the direction of the received signal for each of the other nodes and share a witness. The neighborhood relationship is confirmed only when the directions of all pairs match.



$$rmax \geq dSR \geq ||pR - pS|| - (TR - TS + \Delta t).2vmax - \Delta d$$

r_{max} maximum range of transmission;
d_{SR} distance between nodes transmitter and receiver R S;
$p_S p_R$ current position of the nodes S and R;
T_S, T_R timestamps sending and receiving message;
Δt max error in the synchronization of clocks;
Δd max error in the positioning of nodes;
v_{max} speed max nodes;

If the formula is not checked against dAB ⇒ possible wormhole AB.

D. Module Specific Hardware and Time Window

In [5] it is assumed that each node is equipped with special equipment capable of responding immediately to 1-bit.The challenger measures the travel time of the signal with an accurate clock to calculate the distance between the nodes.

Assumed: (0) nodes communicate via radio transmission; two nodes are considered neighbors if they are worn transmission;(1) each node has a clock and local clocks between nodes are loosely synchronized (the difference between two clocks of network nodes is less than 1 second).For a low clock synchronization, the authors refer readers to "Time synchronization in ad hoc networks, K. Romer; (2) Each node is equipped with a specific hardware module that can provide temporary control of the unit transmitting / receiving radio transmissions from the CPU. With this hardware module, a node can receive a single bit, perform a XOR operation on two bits, and then transmit a single bit without involving the CPU of a node; (3) it is not required that the nodes are equipped with a geographic positioning module; (4) nodes are able to generate cryptographic keys to verify signatures, to perform functions of ground (that is to say, accomplish any task required to secure communications);(5) the system operates with a central authority whose role is to control the associations to network and to assign a unique identity to each node; (6) all nodes in the network have either shared secret keys. The proposed technique allows an entity (the checking) to determine an upper bound on its physical distance with another entity (the evidence). It is based on two elements: the fact that light travels at a finite speed (about 30cm by nanosecond), then the fact that current technologies can measure local timings (timings) with an accuracy up to the nanosecond. With these two elements, it is possible from the travel time on a turn signal to derive an upper bound on the physical distance between a checking and a can. It requires several rounds of rapid exchange of bits between the checking and up (several rounds of exchange of bits).Each bit emitted by a first entity is considered a challenge to which each other entity must issue a response on a bit now. For a local measure of time elapsed between the time of issuing the challenge and the response time of reception, the first entity can compute an upper bound of the distance to other entities. The authors propose a variant of the Chaum protocol Brands-called MAD (Mutal Authenticated Distance-bounding). This is a multi-round protocol for estimating a bound securely to the distance between a pair of nodes.

IV. Description of Wormhole Attacks

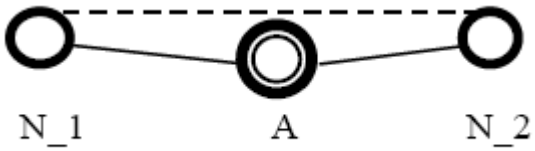


Fig. 1. Wormhole attack conducted by a single attacker

In general the attack by a wormhole (a term referring to wormhole in astronomy that is shortcuts between distant points in space), the traffic part of the network is recorded and relayed to another party network. A wormhole attack can be conducted either by a single node adversary, or by a coalition of opponents. The figure1 illustrates the principle of the attack according to the first model of opponent. We consider an adversary node (denoted A) located in both the direct field of communication between two legitimate nodes (denoted N1 and N2), wherein N1 and N2 are not focused direct communication. By a simple relay control messages N1 to N2 (and vis-versa), the adversary A succeeds in establishing a physical link between N1 and N2 non-existent and he has full control. Indeed, in the following exchanges between N1 and N2, the opponent can either continue the relay of messages through the tunnel is breaking the link

V. Wormhole Attack in OLSR

The attack "wormhole" can strongly influence the topology construction, it can be fatal for many ad hoc routing protocols, particularly proactive routing protocols OLSR that exchange control packets for neighbor discovery and construction of the topology.

Fig. 2 represents an ad hoc network, including a tunnel vortex. When the node A broadcasts its HELLO message the node X (the attacker) copy this message “HELLO” and sends it to node Y through the vortex built. Y receives the HELLO message and replays it in his speech.

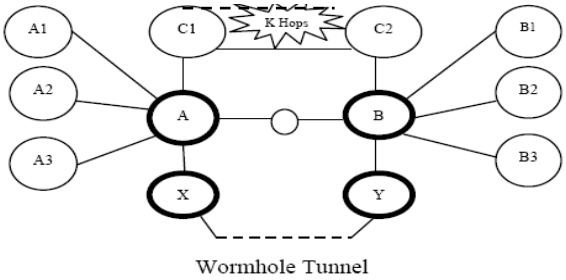


Fig. 2. Wormhole Attacks carried out by two attackers

When the node B receives the message replayed, the node B considers node A as a neighbor 1 hop. After a while, a symmetrical relationship can be established between A and B in the mechanism of OLSR. Once this link is established symmetric, A and B are very likely to choose each other as multipoint relay (MPR), which then leads to an exchange of some topology control (TC) messages and data packets through the wormhole tunnel. In our example of FIG 2.B can expect neighbors to 1-hop of A, which are neighbors of B to a 2-hop that part A. Therefore, B must choose A as MPR neighbors wait for 1-hop of A, then transmission of

erroneous information, this leads to disruption of routing and loss of connectivity.

VI. Detecting Wormhole Attacks

After review and analysis of various existing proposals in the literature on the various solutions level for the attack on the wormhole first, and the advantages and disadvantages of each method on the other hand, we then based on the addition of four posts *"*HELLOreq*, HELLOrep, Probing, ACKprob "*at the OLSR because it does not require time synchronization or location information, especially since it requires no special equipment or complex calculation, and have proposed using the MD5 algorithm and RSA to sign messages.

In this section, we describe our proposal for detecting and preventing the wormhole attack using OLSR as routing protocol. In our approach, nodes initially trying to detect suspicious links part of the wormhole after the audit.

A. Detecting Suspicious Links

The main concept used in the protocol is that of multipoint relays (MPRS). The MPRS are selected nodes which send broadcast messages during the process of flooding. This technique significantly reduces the overhead to messages from a classical flooding mechanism where every node retransmits each message when it receives the first copy of the message. In OLSR, the link state information is generated only by nodes elected as MPRS, and a second optimization is achieved by minimizing the number of control messages flooded in the network as a third optimization, a node MPR must report only links between itself and its selectors. The characteristic of the wormhole attack consists of packet latency relatively longer than the latency of wireless propagation normal to 1-hop.This is usually because the attack of wormhole many routes multi hop are directed toward the wormhole. Increases the burden on single path leading to more general queues delays in the wormhole. However, this is not a sufficient condition for the existence of a wormhole, because the packet transmission and affected by various factors such as congestion. To deduce suspicious links, we define two new packages for control OLSR: ***HELLOreq&HELLOrep***

The message "HELLOreq" replaces the message "HELLO" standard OLSR, and whichever option is chosen, there may be one of two directions. In the standard option, it works like the original message. In an another option uses the HELLO message of request for an explicit response from its neighbors. In this option, when receiving a message HELLOreq, the neighbors must respond with a message HELLOrep.HELLOrep and HELLOreq have exactly the same format of the standard OLSR HELLO. (Figure3)

After each transmission of N HELLO message, a node sends a message HELLOreq. The value of N can be adjusted depending on the level of security. N must be set to a value sufficiently small. When a node receives a HELLOreq, it records the address of the sender and the time i Δi. The default message is HELLO 2s (The transmission interval) in OLSR [6].To avoid overloading the network with too many answers HELLO message, A receiver delay responses of several requests until it is scheduled to send its HELLO message standard.

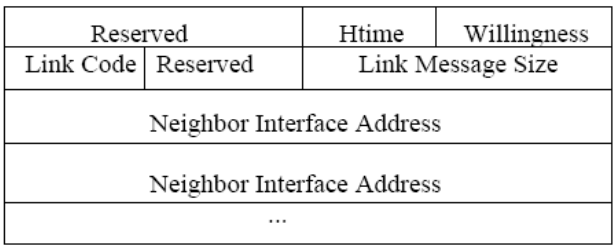


Fig. 3. Datagram message HELLOreq

Reserved: This field should be "0000000000000000".
Htime: Interval of issuance of messages Hreq,
Willigness: to force the passage of a node in MPR
Link Code: Code identifying the type of link (no information, symmetric, asymmetric) between the sender and the interfaces listed ("Neighbor Interface Address").

The figure 4 shows an example of a timing where a cluster of three responses HELLOrep previously received messages HELLOreq. When a node receives a HELLOrep, it checks if HELLOrep contains information relating to each of its applications. If there is no information on his previous requests, the node treats 'HELLOrep' received as a message "HELLO" normal. Otherwise, the node monitors the arrival time of "HELLOrep" is the arrival in its range of expected waiting time. If "HELLOrep" fails in its expected waiting time, the author classifies the node connection between itself and the node that sent the "HELLOrep" as suspect and stopped communicating with this node until the end of the verification procedure of the wormhole.

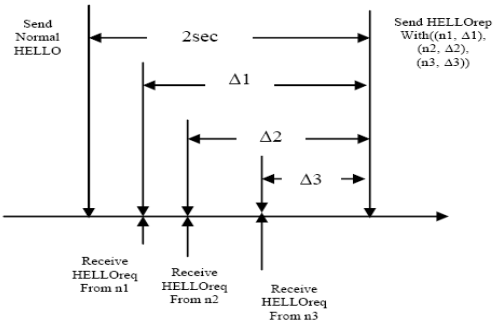


Fig. 4. HELLOrep aggregation

A. Wormhole Verification

After the detection of suspicious links, the origin of "HELLOreq" performs a verification procedure for each link suspect.To this end, two new messages are added to the protocol to detect the wormhole tunnel; a node sends a packet of "Probing" to all of its nodes suspects. When one node receives the packet "Probing" he responds with a message to the sender ACKprob package "Probing" after stopping all transmissions of data packet. The ACKprob also contains the treatment given by the receiver of the package "Probing" until he replied with ACKprob. This information is now used to set a specific timeout. If the node receives a packet of "Probing" do not have any information on the status of the source node, it fails to send the ACKprob and starts collecting the desired information exchanged through "HELLOrep" and "HELLOreq". When the sender of the package "Probing" receives "HELLOreq" instead of

"ACKprob", it immediately sends a package HELLOrep "and initializes a new timeout for this node. The waiting time for other nodes is not changed. If this node sends a packet "Probing" and "ACKprob" at a time, each packet can be grafted another package.(Fig5)

To ensure the safe exchange of a package of "Probing" and "ACKprob". We proposed MD5 and RSA to sign messages. Fig. 6

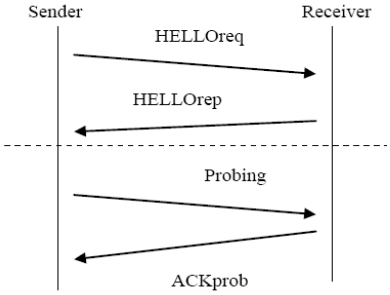


Fig.5. Exchange message to detect the wormhole

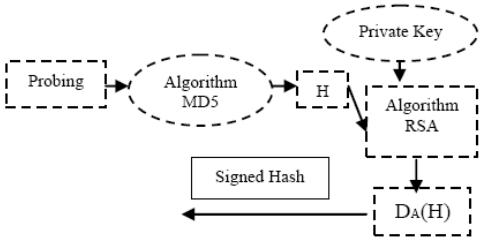


Fig. 6. MD5 and RSA signed messages

Principle:

Input: message of arbitrary length,

Treatment: Apply some operations on the blocks of the message,

Released: Produced as output a 128-bit fingerprint.

With this technique hash it is impossible to produce two messages having the same condensation message. The MD5 algorithm performs the following steps to calculate the condensate from the message:

-Step 1: Add bits of extension. Its new length is congruent to "448" modulos "512".

-Step 2. Update length. The 64-bit representation is added to the result of the first step in getting a data whose total length is a multiple of 512.

-Step 3. Initialize MD buffer size 128 bits with an initial value

A buffer of four words (A, B and C and D) was used to calculate the size of condensate message. Size of each register is 32 bits initialized to the following values in hexadecimal

- Word A: 01 23 45 67
- Word B: 89 ab cd ef
- Word C: fe dc ba 98
- Word D: 76 54 32 10

-Step 4. Process the message in blocks of 16-words

- Main part of the MD5 algorithm.
- Consists mainly of 4 rounds on the message blocks.
- Each round processes a block of 512 bits that mix the contents of the buffer of 128 bits.

-Step 5. Generate a condensate output of 128-bit message.

If the node receives a packet encrypted "Probing", first it decrypts the packet, then verifies the identity of the shipper. If authentication is successful, the node constructs a "ACKprob" which contains the state of the sender. Similarly the node hach "ACKprob" and number before sending it. After receipt, the sender checks the validity of the message "ACKprob" before using the information contient. Again, the author of the verification packet is investigating whether "the ACKprob" has arrived time limit, similar to the procedure of "HELLOrep" and "HELLOreq", the author also decides in this exchange on any suspicious links. To decide whether a suspicious link through a tunnel, the node compares its assessment of the reputation of the other end of the link with the other node evaluation suspicious of his own reputation status:

(Prov, Prov) **:**If the result of the reputation of the remote node is proved and the contents of the encrypted ACKprob is proved, the author concludes that the link between him and the knot does not suspect a wormhole tunnel. The author maintains close relationship with that node and accepts the information from this node.

(Susp, Prov) ou (Prov, Susp) **:**If any two nodes judge the remote node or the contents of "ACKprob" as suspect, the author concludes that the link is always suspect. In that case, the author restarts communication with the node after a time chosen at random. When this period expresses the exchange of packets "Probing" and "ACKprob. If the result of this exchange leads to the conclusion of at least one suspect state, the author treats the link as a tunnel wormhole.

(Susp, Susp) **:**If the reputation of the remote node and the content of the ACKprob are suspect, the author concludes that the link contains a tunnel. Consequently, the author removes the node from the list of neighbors to one-hop neighbors and 2-hop that are one hop to that node. If the suspect node was chosen as MPR, the author moves to a list of nodes forced non-MPR. The author does not use this link, and packets arriving via this link are deleted. If the sender to send packets to the node of the suspect, he must find another way to achieve this node to the exclusion of the link vortex (Wormhole link).If there is no other way for this node. The author expects the exchange process "HELLOreq-HELLOrep" next to discover alternate paths.

B. Timeouts

The value of the *timeout* has to be calculated carefully in order to avoid false decisions. If the *timeout* is set to a too small value, the legitimate nodes can be mistakenly suspected. On the other hand, if the *timeout* is set to a highly large value, it becomes almost hard to detect any wormhole attack. The *timeout* setting is related to whether it can distinguish the normal wireless transmission range of a single hop. *Timeout* can be then defined as follows:

$$\boldsymbol{Timeout} = \frac{\mathbf{2R}}{\mathbf{V}} + \mathbf{Tproc}$$

where R denotes the maximum transmission range of each node or radio coverage. V is the propagation speed of the wireless signal (e.g., the light speed C). In our solution, if a link is regarded as *suspicious*, the link is given another chance to prove its legitimacy rather than being subject to immediate coercive measures. The parameter Tproc denotes the packet processing time and the queuing delays within nodes. Usually, Tproc is hard to be calculated by

formulation as it heavily relies on the topology, the amount of traffic sent/received, and the link conditions (with many collisions or not). In our solution, a sender uses an approximation of receiver's Tproc because it's not using any authentication in HELLOreq-HELLOrep exchange procedure. When the originator sends normal HELLO messages and HELLOreq messages, it records the difference between packet scheduling time and real transmission time. An average of the latest three records is calculated and is used as Tproc in the HELLOreq-HELLOrep exchange procedure. However, an approximation of Tproc is not needed in the *Probing*-ACKprob exchange procedure due to the used end-to-end authentication. Therefore, the sender uses Tproc from the receiver, the difference between the *Probing* packet receiving time and the ACKprob sending time to decide whether there is a wormhole link or not.

VII. Performance Evaluation

In this section, we evaluate the performance of our system using the simulator Glomosim. We generated a number of random topologies with M nodes over a square field; where M ranges from 10 to 50. The square field size is varied from 400x400mto 1500x1500m depending on the network size (i.e., number of nodes). The maximum transmission range of each node is set to 250m. The malicious node pair is selected randomly among the nodes in the formed network. To prevent statistical biases, the presented results are average of 100 simulation runs. Every node, including the malicious nodes, and control messages such as HELLO or TC messages, follow the default settings as in the specifications of the OLSR protocol [6]-[15].

VIII. Result And Discussion

The Fig. A.1, 2,3,4 shows the results of detection Accuracy. Detection Accuracy is measured by the ratio of actual links That Contain wormhole tunnels on the links That Are Deemed suspicious by our solution. The results show that the detection accuracy depends on the correlation between the number of nodes and the length of the tunnel. In a network of 15 nodes, the detection accuracy rarely decreases with increasing length of the tunnel. However, in large networks (eg, nodes 30 and 50), the detection accuracy decreases significantly with increasing length of the tunnel.

Fig. B.1, 2, 3, 4 shows the rate of detection of wormhole link depending on tunnel length for different sizes of network. The tunnel length is the number of hops between nodes malicious. The range of emission is equal to "HELLOreq" 5 (which means that after sending five "HELLO" normal one "HELLOreq" is sent), and the length of the wormhole attack is fixed at 30 seconds. The results show that wormholes are found more in the configuration where the attack is launched on a number of more hop. This result is quite obvious, since through a wormhole tunnel packets are encapsulated and decapsulated repeatedly, leading to more delayed transmissions. In the case of less than three hop, the rate of detection is relatively low.

Fig. C shows the rate of detection of the wormhole connection with different intervals of emission "HELLOreq" and different duration of the attack of the wormhole when the number of nodes is 30. The graph highlights the correlation between the interval and emission data "HELLOreq" and the length of the wormhole attack. If the duration of the attack of the wormhole is shorter than the interval of issue "HELLOreq, the detection rate of the link of the wormhole is poor (less than 0.5). This is because there are nodes that do not meet the redemption process "HELLOreq-HELLOrep.

Our approach shows a good detection rate after two intervals show "HELLOreq. This result demonstrates the impact of the interval of emission "HELLOreq" on the detection time. If the interval of emission "HELLOreq" and long enough, it takes more time to detect the wormhole. Therefore, an application that requires a high degree of security must use small intervals of issue "HELLOreq".

IX. Conclusion

The wormhole attack remains a severe attack and not fully resolved, particularly in a configuration of ad hoc network where OLSR is used as the routing protocol.

Wormhole attacks are severe, which can easily be launched, even in networks of confidentiality and authenticity. In the article we have proposed a more effective method for detecting and preventing attacks Wormholes in OLSR. Its detection principle is based on the use of four messages "HELLOreq, HELLOrep, Probing, ACKprob." The solution is easy to deploy, and does not require time synchronization or location information, nor does it require any special hardware or complex calculation. The performance of this approach show a high detection rate under various scenarios.

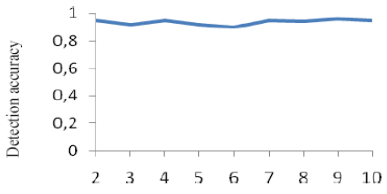


Fig. A.1 Wormhole link detection accuracy for different network sizes (HELLOreq emission interval N=5,number of nodes=15, Wormhole attack duration = 30 sec)

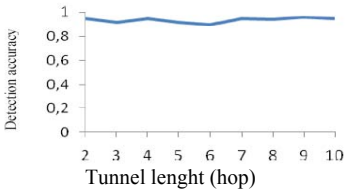


Fig. A.2 Wormhole link detection accuracy for different network sizes (HELLOreq emission interval N=5,number of nodes=30, Wormhole attack duration = 30 sec)

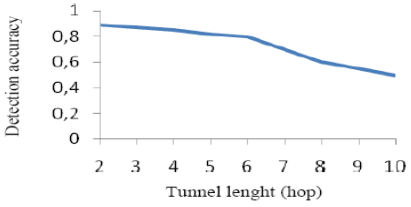


Fig. A.3 Wormhole link detection accuracy for different network sizes (HELLOreq emission interval N=5,number of nodes=40, Wormhole attack duration = 30 sec)

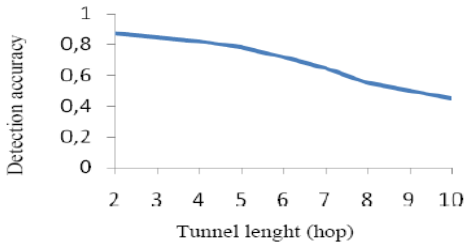


Fig. A.4 Wormhole link detection accuracy for different network sizes (HELLOreq emission interval N=5,number of nodes=50, Wormhole attack duration = 30 sec)

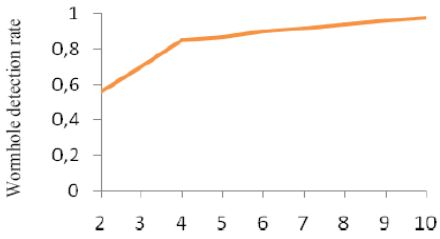


Fig. B.1 Wormhole link detection rate for different network sizes (HELLOreq emission interval N=5,number of nodes=15, Wormhole attack duration = 30 sec)

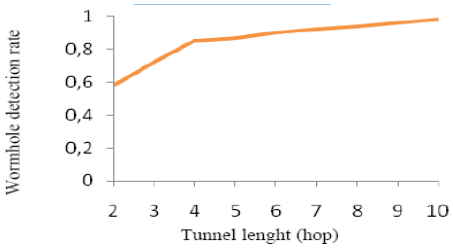


Fig. B.2 Wormhole link detection rate for different network sizes (HELLOreq emission interval N=5,number of nodes=30, Wormhole attack duration = 30 sec)

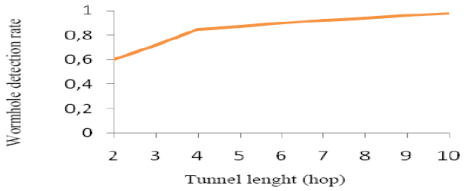


Fig. B.3 Wormhole link detection rate for different network sizes (HELLOreq emission interval N=5,number of nodes=40, Wormhole attack duration = 30 sec)

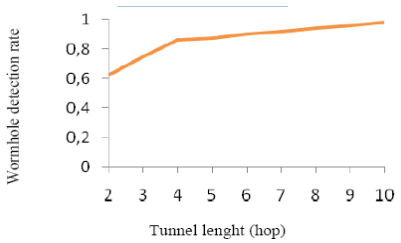


Fig. B.4 Wormhole link detection rate for different network sizes (HELLOreq emission interval N=5,number of nodes=50, Wormhole attack duration = 30 sec)

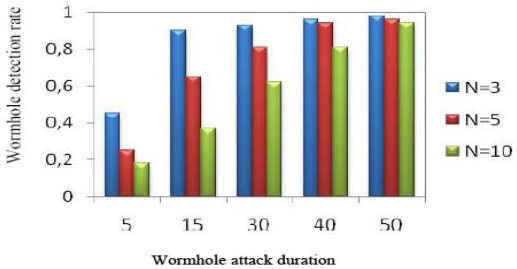


Fig. C. Wormhole link detection rate for different HELLOreq emission interval and different wormhole attack durations (network size = 30 node).

REFERENCES

[1] Y. Huang and W. Lee, "A cooperative intrusion detection system for ad hoc networks," In *Proc. of 1st ACM Workshop on security of Ad hoc and Sensor Networks, Fairfax*, VA, USA, 2003.

[2] Etude des vulnerabilities du protocole de routage OLSR, Céline Burgod, 2007

[3] Y. C. Hu, A. Perrig, and D. B. Johnson, "Wormhole Attacks in Wireless Networks," *IEEE JSAC*, vol. 24, no. 2, pp. 370–80.

[4] L. Hu and D. Evans, "Using Directional Antennas to Prevent Wormhole Attacks," in *Proc. Network and Distrib. Sys. Sec. Symp*, San Diego, CA, 2004.

[5] S. apkun, L. Buttyán, and J.-P. Hubaux, "Sector: secure tracking of node encounters in multi hop wireless networks," in *Proc. of the 1st ACM workshop on Security of ad hoc and sensor networks*, (New York, NY, USA), pp. 21-32, 2003.

[6] T. Clausen and P. Jacquet.Optimized link state routing protocol .http://ietf.org/internet-drafts /draft-ietf-manet-olsr-11.txt, July 2003.

[7] Detecting and Avoiding Wormhole Attacks in Wireless Ad Hoc Networks. FaridNait-Abdesselam, BrahimBensaou, TarikTaleb.

[8] S. Capkun, L. Buttyan, and J.-P.Hubaux, "SECTOR: Secure Tracking of Node Encounters in Multihop Wireless Networks," in *Proc. ACM Wksp. Sec. of Ad Hoc andSensor Networks*, 2003.

[9] L. Qian, N. Song, and X. Li, "Detecting and Locating Wormhole Attacks in Wireless Ad Hoc Networks through Statistical Analysis of Multi-path," in *Proc. IEEEWCNC, New Orleans*, 2005.

[10] H. S. Chiu and K.S. Lui, "DelPHI: Wormhole Detection Mechanism for Ad Hoc Wireless Networks," in *Proc. Int'l.Symp.Wireless Pervasive Comp*, Phuket, Thailand, 2006.

[11] L. Lazoset al, "Preventing Wormhole Attacks on Wireless Ad Hoc Networks: A Graph Theoretic Approach," in *Proc. IEEE WCNC*, New Orleans, 2005.

[12] S. Corson and J. Macker, "Mobile ad hoc networking (manet): Routing protocol performance issues and evaluation consideration," *Request for Comments (Informational*, 1999.

[13] I. Khalil, S. Bagchi, and N. B. Shroff, "LITEWORP: A Lightweight Countermeasure for the Wormhole Attack in Multihop Wireless Networks," in *Proc. Int'l. Conf. DependableSys.and Networks*, Yokohama, Japan, 2005.

[14] Y. Zhang et al, "Location-Based Compromise-Tolerant Security Mechanisms for Wireless Sensor Networks," *IEEE JSAC*, vol. 24, no. 2, pp. 247–60. 2006.

[15] Y. C. Hu, D. Johnson, and A. Perrig, "Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols," in *Proc. ACM Wksp*. Wireless Sec, San Diego, 2003.

Mohamed Amine Ferrag is PhD student in networks and computer security at University Badji Mokhtar, ANNABA, ALGERIE. He received his bachelor in computer science in 2008 and his master in networks and computer security in June 2010 at University Badji Mokhtar. He is a member of IACSIT International Association of Computer Science and information technology. He currently works in the department of computer and researcher in LRS (Laboratory Network and System) meet the security concerns of mobile social networks under the supervision of Dr. Mehdi NAFAA. (e-mail: mohamed.amine.ferrag@gmail.com)

Mehdi Nafaa is a doctor in computer science. He received his Enginner status in Computer Badji Mokhtar University in 2003, his Master's degree in Computer Science, Poitiers, France in 2005. And his Ph.D in Computer Science University Evry FRANCE. He currently teaches in the Departement of Computer Science University Badji Mokhtar, Annaba, ALGERIA and Head of research laboratory in LRS (Laboratory Network And System). (e-mail: mehdi.nafaa@gmail.com)