OIC-CERT Computer Emergency Response Team

OIC-CERT Journal of Cyber Security
Volume 2, Issue 1 (February 2020)
77 – 86

Securing the OLSR Routing Protocol

Amin Nurian Dehkordi[1], and Fazlollah Adibnia[2]
[1,2]Cert (APA) Center, Yazd University. Yazd, Iran
[1]**apa@offices.yazd.ac.ir,** [2]**fadib@yazd.ac.ir**

ARTICLE INFO

Article History
Received 6 Oct 2018
Received in revised form
15 Aug 2019
Accepted 25 Sep 2019

Keywords:
security, ad hoc networks, trust, OLSR

ABSTRACT

Mobile Ad-hoc networks are self-organized wireless mobile networks that do not rely on any fixed network infrastructure. Due to limited capability including battery, local memory, CPU cycle, any design of protocols in these networks has to consider these limitations. Trust always exists in protocols, which their running are based on cooperation, especially in routing operations between the nodes in these networks. Indeed, these networks can operate properly only when nodes cooperate with each other truly and in a routing operation, which is defined by a standard. In this paper, we propose a method to verify the trust of nodes by their neighbors, while its amount influences the decision about choosing the MPR nodes and causes an improvement in OLSR's routing protocol security. The proposed method brings few modifications and is still compatible with the bare OLSR. We perform an overall evaluation of our proposed method through simulations. Simulation's results indicate performance of our approach while providing effective security.

I. INTRODUCTION

Several routing protocols have been defined for the MANETs [1]. Generally, it is possible to classify routing protocols in MANETs into two classes: reactive and proactive. The reactive protocols such as DSR will find the shortest route by broadcasting a route request only when they require sending data [2], but in proactive protocols, for instance OLSR, each node holds an entire overview of the network topology [3]. Since the usage of MANETs have been increased, in order to benefit from their advantages and apply them in everyday life, and also because of self-organization in these networks, soon it was clarified that the routing protocols security such as OLSR protocol, are the problems in these networks which have never been considered in designs at all. These protocols have been designed on this fact that all of their nodes are correct.

Adnane et al. [7] have proposed a trust-based solution for securing the OLSR Ad hoc routing protocol in three phases. The first phase was the analysis of the implicit trust relations in OLSR protocol. This analysis highlights the possible measures to make OLSR more reliable by exploiting the operations and information already existing in the protocol. To detect misbehaving nodes, they have developed in the second phase, trust-based reasoning by correlating information provided in the OLSR messages received from the network. The integration of this reasoning allows each node to test the consistency of the behavior of other nodes and validate trust relationships established implicitly. Finally, the third phase complements the second by offering two complementary solutions: prevention to resolve certain vulnerabilities of OLSR protocol, and countermeasures to isolate malicious nodes. Trust reasoning in here is, validating neighbors' behavior and

ISSN 2636-9680
eISSN 2682-9266

performance according to OSLR protocol specification. In this model, trust of nodes, which carry out wrong or abnormal behavior and in general do not operate according to OLSR protocol specification, will be reduced. In this paper, we introduce a method to verify the trust of nodes by their neighbors, while its amount influences the decision about choosing the MPR nodes and causes an evolution in OLSR's routing protocol security. On the other hand, considering the networks MANETs nodes limitations in processing capacity, energy and bandwidth an incorrect operation from a node can't always result a malicious node. Because the node did not have enough processing capacity for directing the received package, thus the node has to be given another opportunity to proof its accuracy. The node's record security is calculated by its neighbors' sent packages and old relations in time series, and for computing its security for this moment a time decay function is used.

This paper is organized as follows: Section 2 presents a brief introduction of related works. In Section 3, we introduce the concept of trust management, trust specification language and we introduce the analysis of implicit trust in OLSR. In Section 4 we present the proposed method. In Section 5 the simulation's results will be described.

II. RELATED WORK

In [4], the authors have proposed a protocol, called CONFIDANT, for making misbehavior unattractive; it is based on selective altruism and utilitarianism. It aims at detecting and isolating misbehaving nodes, thus making it unattractive to deny cooperation. Trust relationships and routing decisions are based on experienced, observed, or reported routing and forwarding behavior of other nodes.

Meka et al. [5] have proposed trust-based reputation model for AODV. Reputation is calculated according to the degree of participation in the routing protocol and the information it provides about the network topology.

Ariadne [6] is another secured protocol based on DSR and TESLA: the authors assume that a shared secret key is distributed for a group of trusted nodes using TESLA and that the nodes are synchronized.

Adnane et al. [7] have proposed a trust-based solution for securing the OLSR Ad hoc routing protocol in three phases. OLSR protocol function occurs in three steps: neighborhood discovery, MPR selection, and routing table calculation.

Gadekar et al. [8] have proposed another secured protocol based on OSLR. To detect and mitigate this Node isolation attack, OLSR protocol is modified by improving its MPR selection procedure. This modified OLSR protocol gives better results than Fictitious Node Mechanism.

Madhvi et al. [9] have proposed another secured protocol based on OSLR. The proposed scheme is to observe malicious nodes misbehavior and stop their malicious activities. This protection scheme provides the protection against DoS attack and routing attack and provides secure communication in dynamic network. The infection just in case of security theme is totally removes in network.

III. TRUST MODEL

Trust, trust models and trust management are subjects which researchers have studied in decision-making in distributed and auto-organized applications. Actually, it has not been defined a specific definition for trust, and all researchers have used their own definition of it for their research area. In this work, Yahalom's [10] trust language and notations are used for indicating trust relationship between nodes. Based on this language, trust is some relations, which help to understand interactions between entities such as humans, network's nodes and organizations. When it is saying, we trust node A, it exhibits a confidence, that node

ISSN 2636-9680
eISSN 2682-9266

A will behave in a certain way and will perform some action under certain specific circumstances.

Yahalom's trust language includes two classes: direct trust relations and the derived trust relations as mentioned in [10], the latter being established on recommendations from other entities. Because of energy, bandwidth and processing limitations derived trust, which is established on recommendation from other nodes and aggregation of them, are not considered.

Therefore, the notations are used for the trust languages in this paper are obtained from Yahalom's trust language and as follow:

Each entity is shown by a capital letter A, B.

The trust between A and B is written by **A trust B**; this means that node A trusts node B and is sure that node B is not a malicious node.

When node A mistrusts node B, it is written by **A ¬ trust B**, this means that node A has detected that node B is a malicious node.

OLSR protocol is classified in proactive routing protocols. It discovers the links between network's nodes by using HELLO and TC messages and then it will broadcast the information in MANET. OLSR protocol consists of three steps: neighborhood discovery, MPR nodes selection and routing table calculation. HELLO messages help each node to detect its one-hop and two-hop neighbors. Then it, among its one-hop neighbors, can select its minimum number of nodes (MPRs) enabling it to reach all the two-hop neighbors. The selected neighbors are called MPRs and advertised in the HELLO message with ''mpr'' status.

A. OLSR protocols notations

An OLSR node stores different data about network's topology and its neighborhood:

- $MANET$: the set of the whole MANET nodes.
- $Asym_x$: includes all asymmetric neighbors of node x.
- N_x : the set of symmetric neighbors of node x.
- L_x : includes all neighbors of node x
- $2HN_x$: the set of two-hop neighbors of node x.
- MPR_x : the set of neighbors of node x which have been recognized as MPR, $MPR_x \subseteq N_x$
- $MPRS_x$: the set of nodes selected as MPRs by node x, which are in charge of routing and forwarding the packets sent by x, $MPRS_x \subseteq N_x$.
- RT_x : the routing table of node x.

In OLSR protocol, each node must advertise its presence by diffusing HELLO messages to its MPR and neighbors, periodically. The selected nodes as MPR also have to advertise all nodes, which have selected them as MPR, by TC messages in the whole network, periodically.

- $HELLO$ is the HELLO message generated by node x; it includes the set of the neighbors of x.
- TC_x is the TC message generated by node x. These messages are broadcasted only by MPR nodes in OLSR and in definite validity time inside the whole network.
- $x \xleftarrow{Hello_y} y$ and $x \xleftarrow{TC_y} y$ are the reception of HELLO and TC messages from y by node x, respectively.

OLSR protocol function occurs in three steps: neighborhood discovery, MPR selection, and routing table calculation [7].

Nodes in OLSR protocol advertise their neighbors by sending HELLO messages periodically, through these HELLO messages each node can detect all nodes, which are two-hop away from itself and control the set of $2HN_x$. In addition, each node must, among its one-hop neighbors, select minimum number of symmetrical neighbors nodes (MPR) enabling it to reach all $2HN_x$ nodes. A node can obtain $MPRS_x$ set by receiving HELLO messages, and by

ISSN 2636-9680
eISSN 2682-9266

observing the present MPR nodes in the messages.

The defined threshold for trust can take different levels in various situations according to the requested service and the mobility degree of the network. The level, which is shown by θ, $0 \leq \theta \leq 1$ is always and is used to detect malicious nodes. On the other hand, if a node evaluates the trust level of other node less than θ, this node will be known as malicious node and will be hold in trust table from the node. Particularly, the bigger value for θ indicates a more trustful network with low efficiency. It is possible to obtain a adequate status between the security and the efficiency of the network by changing the value of θ.

At first, by detecting the asymmetrical neighbors, trust on these nodes initializes less than the initialized threshold. Therefore, we will have $A \in Asym_B \Rightarrow B \neg trust\ A$, and after a node becomes a symmetrical neighbor, trust on it will initialize to minimum value of trust.

$$A \xleftarrow{Hello_B} B, A \in Asym_B \Longrightarrow A\ trust\ B,$$
$$N_A = N_A \cup B, 2HN_A = 2HN_A \bigcup (N_B - A) \quad (1)$$

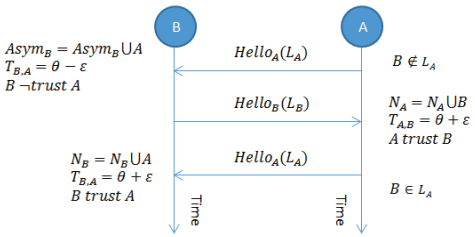

Fig. 1: Trust relationship creating in discovering neighbors.

In **Fig. 1**, at first while between node A and B is not any trust relation, node A sends a $HELLO_A$ message. After receiving this message by node B, a new simplex link is defined for B and the initialized trust to A will be equal to $\theta - \varepsilon$, while ε is much less than θ. After receiving the $HELLO_B$ message by node A and observing itself as a neighbor from node B, a symmetric link will be formed between A and B, because B and A have received $HELLO_A$ and $HELLO_B$, respectively. In this state, a trust relation will be established between these two nodes (A, B) by changing the link type to symmetric and initialized trust will be set θ.

B. MPR selection

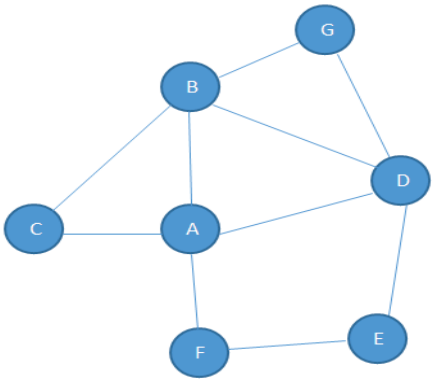

Fig. 2: Node A selects node D as its MPR.

After the detection of one-hop and two-hop neighbors, each node have to, among its one-hop neighbors, select the minimum number of nodes enabling it to reach all the two-hop neighbors. All selected nodes as MPR are advertised to neighbors by HELLO message. For instance, in **Fig. 2** it is only necessary that node A selects node D as its MPR.

When a node is selected as MPR, it will advertise the nodes, which have selected it as MPR, by TC messages in the whole network periodically. TC messages contain the necessary topological information for computing routes to the whole network and will only broadcast by MPRs in the whole network. A node can build its set of topologies and establish its routing table by receiving TC messages, and always the computed routes from one node to other one include MPR nodes across the route. In the presented trust model, choosing node D as MPR by node A means that node A trusts node D, which is to say:

$$\forall x \in MPR_A : A\ trust\ x \quad (2)$$

Selected MPR nodes have to choose their MPR nodes likewise, thus a chain of

ISSN 2636-9680
eISSN 2682-9266

trust between the MPR nodes will create. Surely, success in this approach does not only depend on selecting the correct local MPR nodes but it depends on selecting correct MPR nodes by its neighbor, as well. Therefore, each node has to trust its MPR's selection, either.

C. Routing table calculation

For computing the routing table, which is the result of the OLSR protocol, TC messages are broadcasted in the whole network. The TC message sender advertises that, which nodes have selected it as their MPR node. TC messages help each node to create the network topology from its own point of view and calculate its own routing table. Moreover, if a node is not chosen as an MPR node by its neighbors, its set of $MPRS_x$ will be empty and will not send any TC message. Every node in the network has topology information that is based on received TC messages, stores the information related to every MPR node in the network. Based on this information, the routing table will be calculated. RT routing table is shown as:

$$\forall z \in MANET\ \exists y \in MPR_x \Rightarrow \exists T \in RT_x, T = (z, y, N, I) \quad (3)$$

Each entry in RT table consists of (z, y, N, I), and specifies that the node identified by z is located N hops away from the local node. The symmetric neighbor node, which is identified by y, is the next hop node in the route to z. From the trust point of view, the computation of the shortest path between x and z through the MPR y means that x trusts y for the routing towards z. Hence, if $T = (z, y, N, I)$ is an entry in RT routing table than:

$$\forall T \in RT_x \Rightarrow x\ trust\ y \quad (4)$$

In addition, in routing table only a route is calculated towards each destination node which is the shortest path that starts from the MPR node. The inherent risk in choosing only one route towards any destination is to choose a misbehaving node as a router. Thus, an attacker can put itself between sender and receiver nodes and disrupts protocol operation by giving false information to the neighbors. Finally, in this model selecting y as x's MPR not only implies that x trusts y, but also trusts all y's MPR nodes and as result trusts all selected routes by y, as well.

D. Trust Reasoning

In this paper, it is assumed that when a packet is sent by a node, all of its neighbors will receive it correctly. Trust reasoning in here is, validating neighbors' behavior and performance according to OSLR protocol specification. In this model, trust of nodes, which carry out wrong or abnormal behavior and in general do not operate according to OLSR protocol specification, will be reduced. Therefore, by passing the time each node observes its neighbors' behavior and stores for each of them N_{neg} and N_{all} values, which are the numbers of observed misbehavior and total behavior respectively. If a node shows misbehavior, then it will increase its N_{neg}. It is obvious that $N_{all} - N_{neg}$ is the observed correct behavior. The definition of is:

$$T_{A,B}^{T_k} = \frac{N_{all}(t_k) - N_{neg}(t_k)}{N_{all}(t_k)} \quad (5)$$

IV. PROPOSED METHOD

Fig. 3 shows algorithm flowchart of the proposed method. This section introduces that how a node can detect malicious nodes by employing the received information from the network and reasoning between them. Detection of abnormal behavior includes verification of consistency between OLSR messages and trust-based reasoning that can be carried out by each node in the network. This is a continuous process which will start from reception of first HELLO and TC messages and will take part in calculating routing table. In other words, a continuous

ISSN 2636-9680
eISSN 2682-9266

and recursive checking of trust properties have to be performed, in order to validate all information received from the network. By using concept of trust, it is possible to change the mentioned properties in above to design a mistrust reasoning, so a node is able to protect itself from malicious nodes.

A. Validation in MPR selection

Selection of MPR nodes is the most important phase in OLSR protocol. Nodes get access to the network through their MPRs and this causes them to be known by the whole nodes of network. In OLSR protocol there is not any way to verify the MPR behavior. This vulnerability is exploited by attackers which try to be selected as MPR by a target node and through this, control the target node input–output messages [11]. The most serious reason of vulnerability in MPR selection is in selecting of nodes; because only degree of reachability to two-hop nodes is important and an attacker is able to give wrong information which cannot be verified [7]. Each node has to use the trust concept to have control over its MPR nodes. Based on OLSR protocol specifications, correct behavior of an MPR regarding to routing is definite by two operations: producing TC messages and forwarding data packets and TC messages of nodes which have selected it as their MPR. If a node can validate this and confirm these functions based on MPR's behavior, then a trust relationship will be created correctly, and the node can operate as MPR. Otherwise, if it is not possible for a node to confirm these two functions and does not obtain enough trust, it has to delete that node from its MPR nodes and find other one among other trustful nodes. Hence, to achieve this goal a blacklist is employed for the selected MPRs that the malicious node will be added to this blacklist. Nodes in the blacklist will not be selected as MPR in the future, but after an expiration time the node will be remove from the blacklist and will have a new chance to be selected as MPR again.

If an MPR node like y has generated false TC messages, and nodes, which use it as MPR node, do not advertise this, then trust to this will be decreased, it has to be deleted from MPR nodes set and has to be inserted to the black list and alternative node or nodes has to be selected as MPR nodes.

If a y's selected MPR does not forward data packets and TC messages, then trust to this node has to be decreased and be deleted from the MPR nodes set and be inserted to the blacklist. Also, alternative node or nodes have to be selected as MPR nodes.

ISSN 2636-9680
eISSN 2682-9266

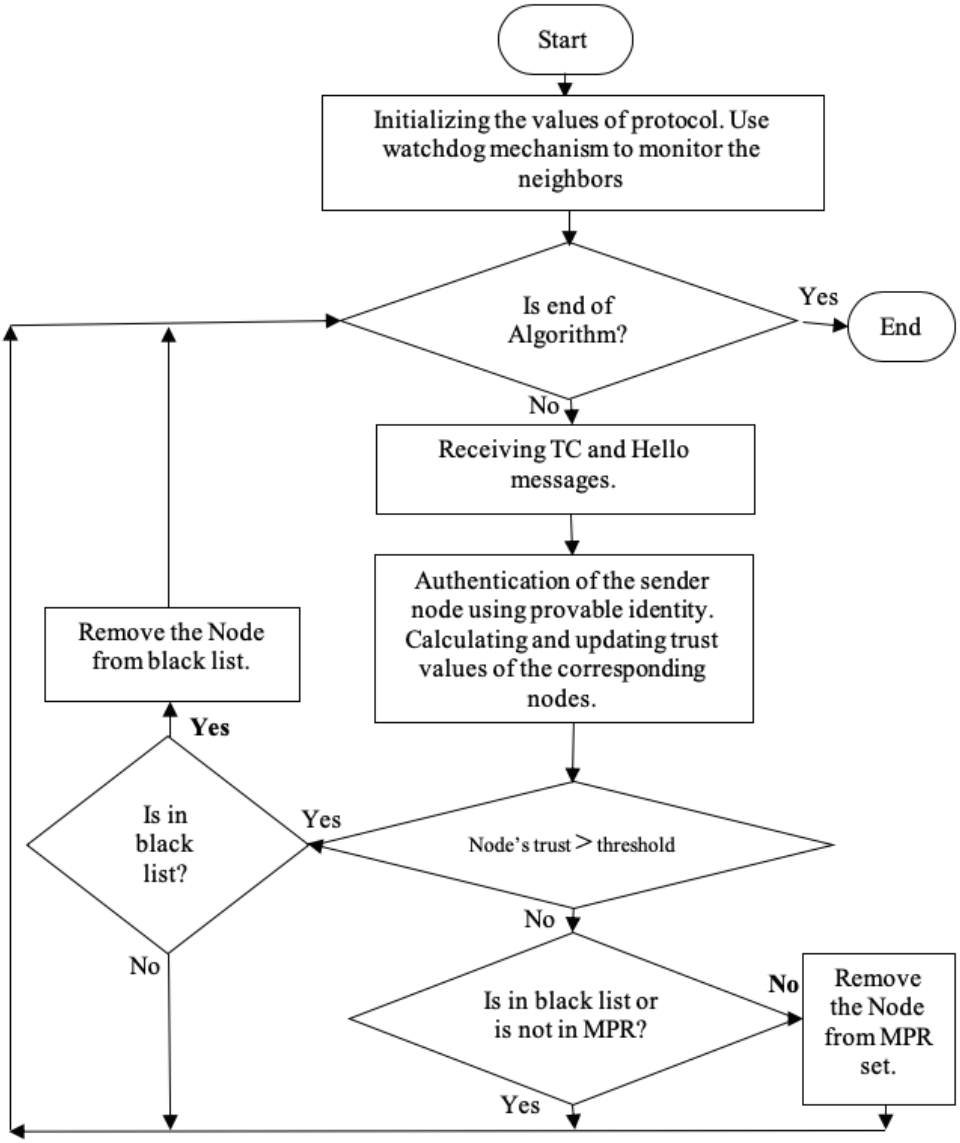

Fig. 3: The proposed method.

ISSN 2636-9680
eISSN 2682-9266

V. SIMULATIONS AND RESULTS

In **TABLE 1**, the proposed method are compared with OLSR protocol. In the proposed method, it is possible to define the required security level for each connection by changing the threshold of it. For example, a multimedia and secret connection needs a high security route and as result a higher threshold in comparison with a file sharing connection. On the other hand, routing overhead in the proposed is higher than OLSR protocol. Authentication of nodes and being confidence about their ID in both methods is performed by using provable identity mechanism. None of these methods needs a centralized entity for operating and they are still compatible with OLSR protocol. Suggestions approach, which is used in credit systems, includes receiving trust value as a suggestion from other nodes about a special node.

TABLE 1: Explanation of the Main KSA Descriptor Sections

	OLSR Protocol	Proposed Method
Security Mechanism	None	Based on trust
Trust history	None	Have
Routing Overhead	Minimum	High
Qualifying nodes origin	None	Provable identity and OLSR protocol
Protocol compatible with OLSR	Yes	Yes

For simulation, NS2 simulator is used. In the simulations, MANETs is composed from 50 nodes which are placed in a flat network with the dimensions 500x500 square meters randomly. In addition, a node's range which has been identified as a step is 250m. We have considered that nodes are not mobile, due to allow the attacker to do its attack over time and also the threshold value is initialized to 0.8.

The attacker node is selected randomly and then it will perform its attack's scenario. **Fig. 4** shows the rate that a malicious node is detected by its neighbors. While, one of the basic assumptions about OLSR protocol is that the whole nodes of network are correct, any security mechanism for protection against malicious nodes are used, and all attacks from malicious nodes will be done successfully. The OLSR method and proposed method have same results in Simulation number 5, because two methods have the same behavior in this number.

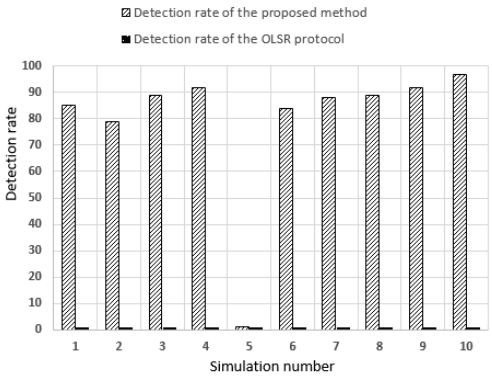

Fig. 4: Comparison the detection rate of the proposed method with OLSR protocol.

In **Fig. 5** is presented the evaluated trust value of the proposed method and Adnane's method [14]. The simulations, which have been done, are in an identical state for both methods and each curve shows the evaluated trust value by the first neighbor of the malicious node.

ISSN 2636-9680
eISSN 2682-9266

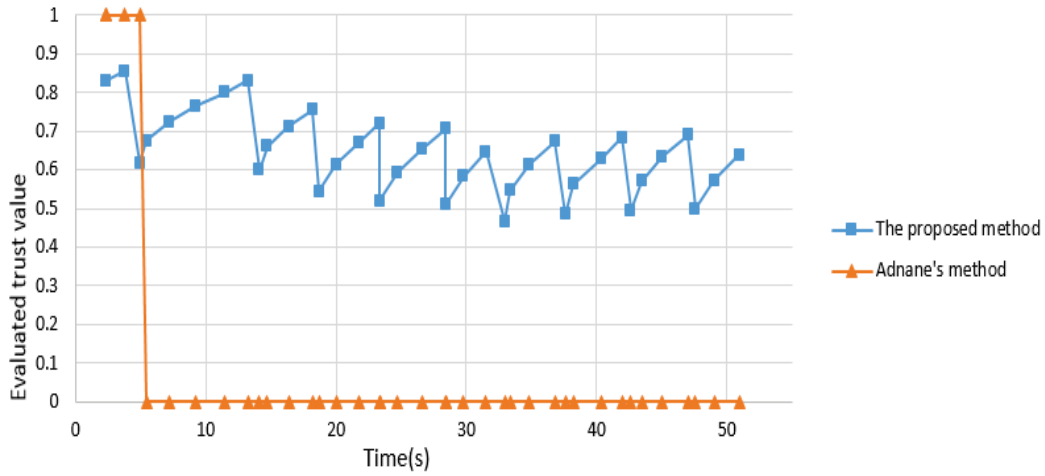

Fig. 5: Evaluated trust value by the first neighbor.

VI. CONCLUSION

It is possible to calculate the trust value of each node in the network by monitoring the network, analyzing received information from neighbors and filtering them. Moreover, by storing and comparing the messages, it is possible to detect false relations and malicious nodes from chain of messages. This solution gives the possibility to use a memorial method in OLSR routing protocol to calculate trust of a node.

The proposed method unlike Adnane's method creates its trust relations by calculating the trust history of a node continuously. The simulations, which have been done, are in an identical state for both methods and each curve shows the evaluated trust value by the first neighbor of the malicious node. The simulations have been presented effectiveness of the proposed method in detecting malicious nodes.

VII. REFERENCES

[1] A. Boukerche, et al., "Routing protocols in ad hoc networks: A survey", *Computer Networks*, 2011.

[2] D.B. Johnson, D.A. Maltz, J. Broch, "DSR: the dynamic source routing protocol for multi-hop wireless ad hoc networks," in: C.E. Perkins (Ed.), *Ad Hoc Networking*, Addison-Wesley, 139–172, 2001.

[3] T. Clausen, P. Jacquet, "Optimized Link State Routing Protocol OLSR," IETF RFC-3626, 2003.

[4] S. Buchegger, J-Y. Le Boudec, "Performance analysis of the confidant protocol: cooperation of nodes – fairness. Dynamic Ad-hoc networks," *Proceedings of IEEE/ACM Symposium on Mobile Ad Hoc Networking and Computing (MobiHOC)*, IEEE , 2002.

[5] K. Meka, M. Virendra, S. Upadhyaya, "Trust based routing decisions in mobile ad- hoc networks," In: *Workshop on Secure Knowledge Management (SKM)*, 2006.

[6] Y. Hu, YA. Perrig, D. Johnson, "Ariadne: a secure on-demand routing protocol for ad hoc networks," *Wireless Networks*, vol. 11, Kluwer Academic Publishers, 21–38, 2002.

[7] A. Adnane, C. Bidan, CR. Timóteo, "Trust-based security for the OLSR routing protocol," *Computer Communication*, 2013.

[8] S. Gadekar, S. Kadam, "Secure optimized link state routing (OLSR) protocol against node isolation attack," *IEEE International Conf. on Power, Control, Signals and Instrumentation Engineering (ICPCSI),* Chennai, India, 2017.

ISSN 2636-9680
eISSN 2682-9266

[9] C. Mahdvi, P. Bhanu, "Prevention of DOS and routing attack in OLSR under MANET," *International Journal of Engineering Science and Computing*, Vol. 7, No. 4, 2017.

[10] R. Yahalom, B. Klein, T. Beth, "Trust relationships in secure systems – a distributed authentication perspective," In: *SP'93: Proceedings of the 1993 IEEE Symposium on Security and Privacy, IEEE Computer Society*, Washington, USA 150–164, 1993.

[11] L. Buttyan, J-P. Hubaux, "Nuglets: A virtual currency to stimulate cooperation in self-organized mobile ad hoc networks," *Proc. of Technical Report DSC/2001/001, Swiss Federal Institute of Technology – Lausanne, Department of Communication Systems*, 2001.

.

ISSN 2636-9680
eISSN 2682-9266