Extenuate the DOS Attacks in OLSR Protocol using Novel Trust Management Method

[1] Ms. Dhivya Bharathi V, [2]Mrs.Sagarika Behera

[1] Final year, M.Tech in Computer Network and Engineering,
[2] Associate Professor, Computer Science Department
[1] CMR Institute of Technology, Bangalore, India

***Abstract*— Mobile Ad-Hoc Networks (MANET) mainly specified for routing efficiency, the resulting protocols tend to be vulnerable to various attacks. In this network, an application contains very sensitive and secret communication since the MANET is in dynamic nature to provide a secure data transmission is difficult. A huge number of methods have been proposed for different types of attacks, however, these methods compromise routing efficiency or network overload. The DOS attack against the Optimized Link State Routing protocol (OLSR) known as the node isolation attack exist when topological information of the network is exploited by an attacker who is able to isolate the victim from the network and deny communication. In this paper, we introduce a novel Trust management approach to OLSR protocol knows as TOLSR to defend the OLSR protocol from node isolation attack Through extensive experimentation we demonstrate that the proposed method prevents more of attacks, the reduces the traffic overload and increases the performance. Lastly, we suggest that this type of solution can be used to other attacks.**

***Index Terms*— MANET; DOS; OLSR; Trust Management**

I. INTRODUCTION (HEADING 1)

A MANET is a collection of mobile nodes which is able to exchange the data remotely with every other node without using predefined centralized system. Sending packets from one device to some other is achieved via a sequence of intermediate nodes. Huge routing algorithms exist for network packets transmission. Generally, these algorithms can be ordered into two major classifications: Reactive routing and proactive routing protocols. In the case of proactive routing protocol, every node in the network will have routing information in the routing table in order to transmit the packet from source node to destination node and constantly updating of routing tables so it is also called a Table-driven routing protocol. It contains the information about the number hops between source and destination, generation of the new sequence number and destination address with optimal path route for example, DSDV and OLSR

In the Reactive routing protocol, routes are determined on demand by using flooding mechanism so routing table is not required. This protocol finds the route in an on-demand manner to transmit the packets it chooses the optimal path between source and destination by using route request (RREQ) packets through the network such as DSR and AODV. In to the account of routing algorithm, Mobile Ad-hoc Network have important requirement and few elements in its success and capable of having all the nodes information in the network. These algorithms are quite different from the standardised routing which is used in the standard network due to the dynamic change in the network topology. There will be frequent changes in the route between sources and destination due to link failure or intermediate nodes dynamically change their position and these nodes can join or quit the network.

The proactive routing protocols is the Optimized Link State Routing protocol is mostly used in present days since it has quite efficient bandwidth utilization and also route path calculation. It exposed to the possibility of being attacked by various method. As OLSR depends on process of working together in the network and due to single malicious node can damage the routes. In this paper using Trust Management approach in order to improve the performance of the OLSR protocol and to eliminate attacker node in the network

II. BACKGROUND AND RELATED WORK

A. OLSR Protocol Overview

OLSR is a table driven protocol. That maintains essential information of all possible destinations among the network and best path routing to it, quite efficient in bandwidth utilization and also path computation. In LSP, each node increase the size of the spanning tree and each node can obtain the complete information in the network topology. the importance of the optimization is based on totally upon subset of 1 hop node, referred to as multi point relay(MPR) that are specific as forwarding agents for managing the packets in the course of the network. MPR's are selected through a node as a subset of its 1-hop of its next node, such that the MPR broadcasting of all of its 2--hop neighbors. by minimizing its MPR selections, a node is able of transmitting messages to all 2-hop acquaintances with minimal duplication. thus, both topologies control messages and information are forwarded by this minimal MPR set, allowing for fewer duplicate messages even as preserving community-wide coverage.

There are 2 types of message used in OLSR: HELLO message and TC. The HELLO message, which contains the information of neighbor node, is broadcast to all nodes in the network. Any node which could pay attention the broadcast and reciprocate again to the sender is classed as a 1-hop neighbor. Therefore, each node requires its sectional topology up to a 2-hop range. In addition, OLSR desire for that all nodes preferred upon as MPRs periodically notifies TC message listing all nodes which have selected the sender as its MPR. These control messages are generated through the MPR outstanding-network, lowering average

network traffic. On each the HELLO and TC messages, it gets. It then calculates and saves, for each node finds the shortest distance (The minimal required hops between the source and the destination) among itself and one of the destination node MPRs ; hence, the shortest route to the destination.

B. DOS Attack

A DoS attack is an attack which reduces the performance of the machine or network, making it unable to reach to its intended users. This attack achieves by flooding huge number of ping packets which leads to more traffic, or sending it information that triggers a crash. The DoS attack prevents legitimate users to the service or resource they expected. Victims of DoS attacks usually prefer the web servers of high-profile organizations such as banking, commerce, and media companies, or public sector and trade organizations. Though DoS attacks typically result in the theft or loss of significant information or other assets, they can lost the victim confidential details There are several levels of DoS attacks but most frequently used is flood attack by sending ping message to crashing network. This attack occur when the system receives too much traffic for the server to buffer, causing them to slow down and eventually stop

C. About Node Isolation attack

DOS attack against OLSR called as node isolation attack. In this attack, an attacker makes use of the fact that the victim a minimal MPR set to be able to cover the existence of the victim within the network. The attackers, which have to be located within broadcast distance of the victim, advertise a fake HELLO, a message claiming to be in close proximity to the victim's entire 2-hop neighbor node. Also, a fictitious node is broadcast, giving the attacker an advantage over other feasible valid legitimacy for an individual for MPR selection. Knowledge of the victim's 2-hop neighbor nodes is readily accessible by way of inspecting TC messages of the victim's 1-hop neighbor node, a list of which may be built directly from the HELLO message broadcast via the victim himself. MPR selection rules would cause the victim to exclusively choose the attacker as its sole MPR, as it is the minimal set that enables for coverage of all the victim's 2-hop nodes

DOS is now straightforward. The attacker can isolate the victim simply by not including the victim in its TC message. In essence, the attacker refrains from notifying the network that the victim can be reached through it, and because no other node advertises a path to the victim, it is isolated. Other nodes, not seeing link information to the victim, would conclude that it has left the network, and remove its address from their routing tables. Although nodes 1- and 2-hops from the victim would continue to exchange information with it, they will not propagate that information further as they were not designated as its MPR.

D. Related works

[Kannhavong et al. tries to reduce the problem of colluding attackers. By modifying the HELLO msg to include all 2-hop neighbors node, a node can find current contradictions among messages, as a result figuring out an attack. Of course, as the authors themselves noted, it's far difficult to distinguish among contradictions which occur due to an attack instead of those resulting from topology modifications. In addition, such contradictions identify an attack however fail to discover the malicious mode in the network.

Raffo et al suggest a mechanism to enhance the security for an OLSR routing protocol against outside attackers. In their solution, each node signs its HELLO message and TC . These signatures are later employed by others to show their own HELLO and TC messages. The resulting solution prevents devices from maintaining imaginary links with recognized nodes. This solution functions correctly but is costly in terms of overhead; except the standard overhead of OLSR, signing messages requires significant computation, a cumulative factor that grows as the size of the network increase. Another problem is the fact that the network loses its spontaneity as all nodes are required to know each other in advance in order to exchange their public keys. This prevents the network from evolving evidently from the various nodes that appear at a certain location and time, an essential trait of MANETs.

Dhillon present IDS every node calculates non-conformances of Topology Control msg with respect to already known HELLO messages. This solution is most effective under the assumption that HELLO msg can be trusted. In node isolation attack, this HELLO message is the main issue. The authors mention the works of and as a strategy for avoiding spoofing attacks in HELLO messages. But, as we already mentioned, adds overhead to the network, as does by utilizing control messages for confirming the HELLO messages. An extended security to the OLSR is introduced by Adjih et al. A signature and timestamp is joined to every control message. These improvements prevent the modification and falsification of topology data and guarantee the timeliness of every message. This method successfully blocks unauthorized users from joining an OLSR MANET, but cannot prevent attacks launched by compromised genuine key holding nodes.

Tries to validate each node mentioned within HELLO message a node receives. This is accomplished by adding 2 new control messages that are utilized for node verification. After getting a new HELLO message, the would-be victim sends a 2-hop verification request through pre-existing channels to each node claimed by the potential MPR to be its neighbour. In response, the queried nodes reply with their 1-hop neighbour list. If the sender is present in all the reply messages, the node deduces that it's legitimate and can appoint it as MPR if it wishes. Otherwise, an attacker has been known, and also the presence of an attacker node is broadcast to the network. The attacker is subsequently removed from the routing tables throughout the network.

DOS FOLSR that modifies the MRP selection process and adds 2 new control messages. Here as well, confirmation messages are provided by two-hop neighbour nodes, with the node receiving the more number of replies selected as MPR. The authors claim that by not depending on one-hop neighbour node, DOS FOLSR prevents node isolation attacks. Empirical evaluation of DFOLSR's cost is not given, and an attacker falsifying the responses of fictitious 2-hop nodes can render the solution useless. Finding the measures to avoid based on message signing and countermeasures imposed when an attack is detected is that the approach taken by [24]. Every new node in beginning sends its signature, which is later used to approach its messages. When an attack is countermeasures are imposed to isolate attacker nodes and ensure also enabled for sharing the information regarding malicious nodes. This solution generally functions well, but does not handle the case once the attacker joins the network prior to

the victim allowing the attacker to masquerade as the victim by sending wrong signature initiation information. In addition, a fake node sending HELLO messages (with wrong signature initiation data) cannot be detected.

In Suresh investigate the illegal attack in OLSR protocol based on MANETs. They introduce a method called Forced MPR switching which needs that a node having a one MPR intermittently change its MPR selection so, eliminating the required pre-condition for the isolation attack among the nodes. This methodology may cause a legitimate network to temporarily fragment and is further limited because mitigation can only occur after the attack has commenced. GID & Prevention and Intrusion Detection & Adaptive Response mechanism are examples of using Intrusion Detection System for solving MANET attack vectors.

In Existing system recommended a solution to prevent the OLSR protocol from the node isolation attack by use the same strategy used by the attacker itself. Through lot of experimentation and demonstrate that prevents attacks, and the overhead required drastically reduces the network size increases and they suggested that this type of solution can be extended to other similar DOS attacks on OLSR .Disadvantage of this method is the DCFM is only in that all the information used to protect the MANET stems from the victim's internal knowledge.

III. PROPOSED SYSTEM

1. Architectural Diagram

There are many routing protocols have been proposed for mobile ad-hoc network such as OLSR, DSDV, GSV and STAR so on. In the proposed system, making few assumptions and establish the network model of Trust OLSR (TOLSR). Main focus is to providing security for routing protocol in the network layer instead of link layer. Initial Procedures are

a. Each node in the network has the capable to collect the information about neighbors.
b. Each node in the network can broadcast HELLO message to its neighbors
c. Select the MPR selector
d. Choose the MPR selector set
e. TC message – updates the neighbor table information often

In Trust management approach it is also called as "**Trusted OLSR**" [TOLSR], this design as shown in the fig:1 is prepared with monitoring mechanisms or intrusion detection units both in the network layer and application layer in order that one node can observe the behaviors of its 1-hop neighbors. In the network layer, a new node model is designed as the basis of our trust model. The new block added into a node's routing table to check the nodes behavior based on i) Energy ii) Bandwidth and iii) Location By adding the trust model into the routing layer of MANET, saves the time and improves the performance of the network

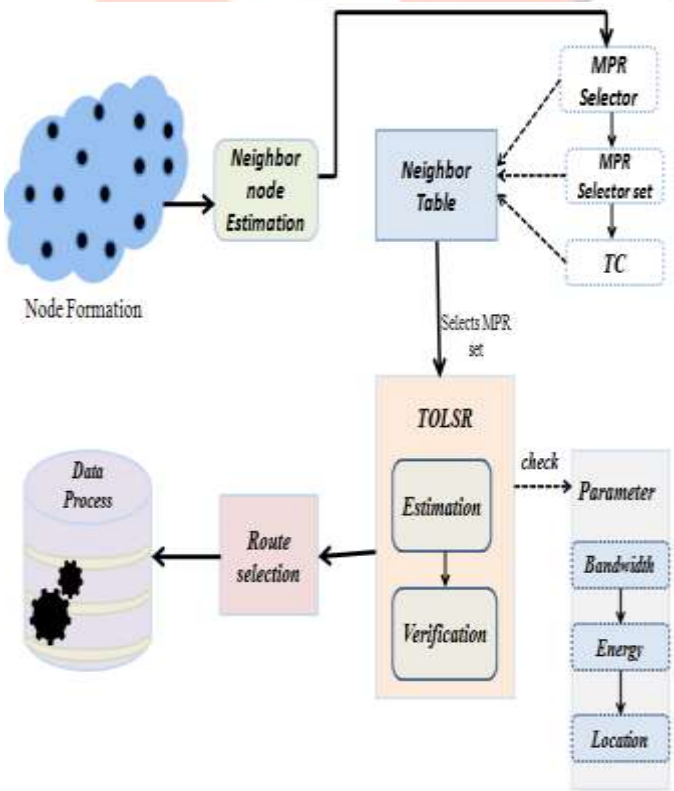

Figure1: Architecture Diagram

Methodologies

1. Network Formation

The first step is to create nodes in the network and since mainly dealing with security; designing the nodes such that victim node must be able to defend the attacker. The malicious node able to check the route and can send the fake reply to the source and

attacker can identify the data packet and it will drop. Victim nodes can make the cooperation with neighbor and can exchange the information, and forwards the data from one to other nodes, and will try to defend from malicious node.

2. *Route Discovery and Neighbor table*

Each node will detect the neighboring nodes. It has a directional and bi-directional link. Each node periodically broadcasts HELLO messages, which contains the information about neighbors and their link status. They will receive from all one-hop neighboring nodes. A HELLO message contains:

- It contain the list of addresses of the neighbors nodes which a valid bi-directional link
- The information about the neighbors which are heard by this node but the link is not validated as bi- directional: if a node finds its own address in a HELLO message, it considers the link to the sender node as bi-directional. This messages Serves Link sensing, allows each node to know the information about the neighbors up to two-hops, On the basis of collected information, each node performs the selection of its multipoint relays.

OLSR protocol uses a technique to reduce message flooding Multipoint Relaying (MPR) and TC.

a. MPR: First it chooses the MPR selector Set which is able to select neighbor nodes which minimize the flooding of broadcast packets and each node chooses its MPRs among its on hop neighbors. The set covers all the nodes that are two hops away. Second, MPR Selector set selects a node as MPR selector where the information required to calculate the multipoint relays, The set of 1-hop neighbors and the two-hop neighbors node and the set of MPRs is able to transmit to all two-hop neighbors.Link between node and it's MPR is bidirectional**.**

In the neighbor table, each and every node collects the information about 1- hop neighbors, the status of the link with the neighbors, and also collects the 2- hop neighbor's information. The link status can be unidirectional, or sometimes bi-directional. The link status as MPR intends that the link with the neighbor node is bi-directional and node is also selects as a MPR by this local node. Each entry in the neighbor table has an associates holding time, upon expiry of which it invalid and removed.

b. TC – Topology control message: periodically forwards a message. it might not be sent if there are no updates and sent earlier if there are updates. It includes MPR Selector Table Sequence number each node maintains a Topology Table based on TC messages Routing Tables are calculated based on Topology tables

3. *Trusted Management Method (TOLSR)*

The Trust Management Method is the main modules in our TOLSR system. In the OLSR routing protocol, adding the new block called TRUST MODEL. It provides the trusted OLSR routing protocol information. Based on trust model, the TOLSR routing protocol contains such procedures as trust Evaluation and trust verification to judging the routing behaviors and nodes behavior and updates. The structure of the flow chart and relationship among these components are shown in figure 2

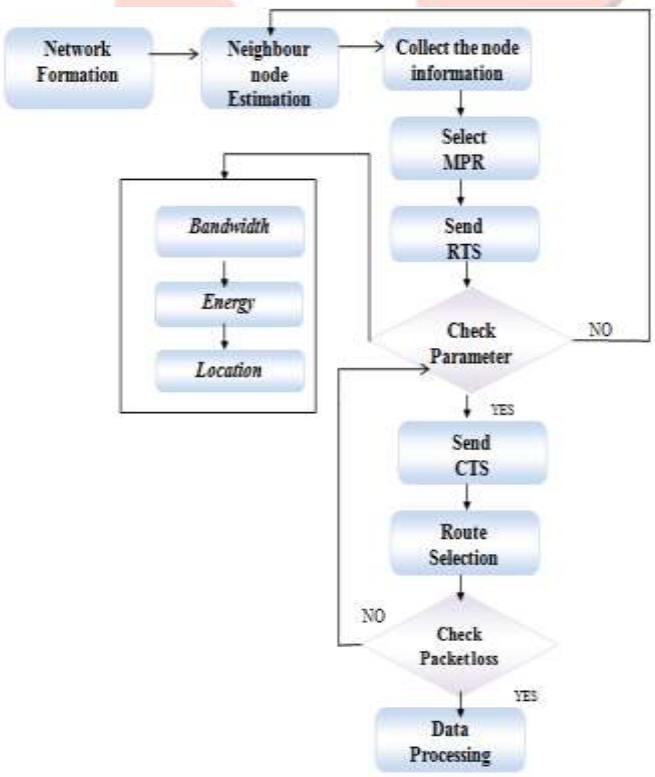

Figure 2: Flow chart

Trust Evaluation and Verification: The proposed Trust OLSR method is an adaptive trust evaluation and verification method. First, it tries to find the trustworthy neighboring node using key factors. There are three main key factors i) Energy ii) Bandwidth iii) Location. If any node's trust value greater than or equal to trust threshold then that neighboring node will be selected for packet transmission. If none node found trustworthy then it finds another way to find and evaluate the trustworthy node for

routing. Commonly, Node makes the transactions with neighboring nodes and gets the indirect information from all neighbors those are situated in its range. Then it updates the database into neighbor node table, and evaluates the trusts and selects the effective node. The node which will be varied from the threshold range and consumes lot of energy and bandwidth it may lead to risky situations. Thus after observation we can conclude that node is Attacker node. In order to improve the performance, prevent the packet loss will choose another route for the packet transmission.

IV. SIMULATION AND RESULT

Simulation:

The implementation of Trusted OLSR is done by using Network Simulator 2 version 2.34. In Mobile Ad-hoc Networks, the nodes will be dynamic in nature where the movements are completely independent of each. The results of these runs were averaged to produce the graphs shown below. The figure 3 provides a summary of the chosen simulation parameter.

```
Total Remained Energy    : 349.101958
Average Remained Energy  : 34.9101958
Energy Difference        : 38.90449912
Packet Delivery Ratio    : 10.840108401084
Average End2End Delay    : 0.522764109375
Average Number of Hops   : 1.15
Control Packet Overhead  : 1438
Throughput               : 69.0347018811918
Data Packets Sent        : 369
Data Packets Received    : 40
Simulation Endtime       : 48.671174184
Total Delivery Time      : 20.910564375
Total Number of Hops     : 46
Dropped Reply Messages   : 3
Maximum Number of Hops   : 4
Minimum Number of Hops   : 1
```

Figure3: Parameters of Network Simulator

Experiment on: Packets Delivery Ratio:

In this experiment, the packet reached metric for the OLSR and TOLSR are measured with node varies 1e+06 to 8e+06 and also 10 to 50 as shown in figure4. The speed of the nodes and the percentage of TOLSR nodes participating in the mobile ad hoc network are varied to compare the results. From the graph figure 5, it is clearly seen that with decreasing the percentage of packet loss in TOLSR nodes in the network, that clearly indicates the performance of the DOS attack is reduced by employing TOLSR method.

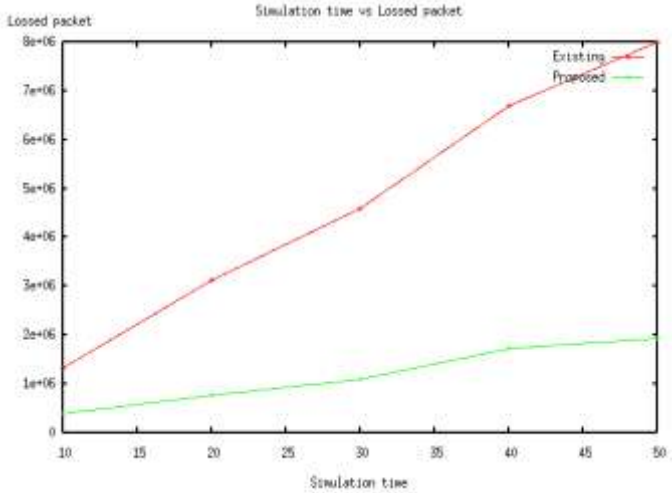

Figure4: Simulation time v/s Packet loss

Experiment on: Network Throughput:

The below figure 5 shows the results of the network throughput of both protocols: OLSR using fictitious node mechanism and Trust OLSR method. This graph shows the dramatic fall in normal reducing the DOS attack in OLSR protocol with previous security mechanism network throughput with increasing percentage of Trust OLSR method

In the case that there are trust nodes in the mobile ad hoc network, both OLSR and TOLSR have almost identical network throughput values. This proves that the TOLSR protocol is as efficient to reduce the DOS attack in the OLSR protocol.

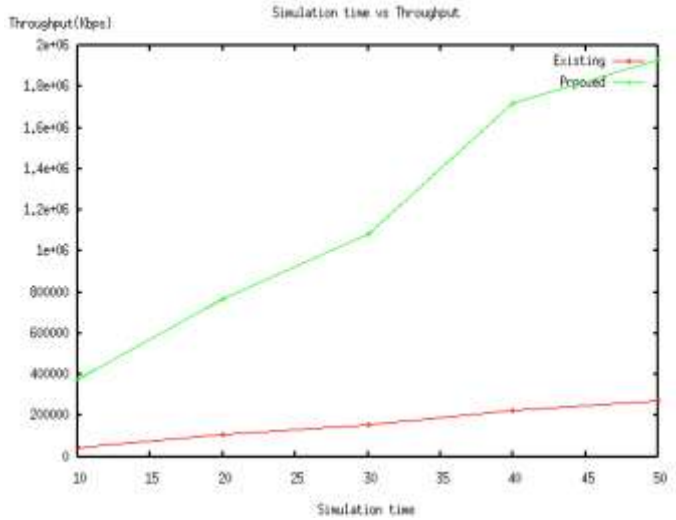

Figure 5: Simulation time v/s Throughput Graph

V. CONCLUSION

In this paper, we have shown a solution called TOLSR method to prevent a node isolation attack. In which the attacker manipulates the victim by employing the attacker as MPR, giving the attacker complete control to exchange he information. Simulation shows that TOLSR successfully prevents the attack, specifically in the scenario in which all nodes in the network are dynamic in nature. In Trusted OLSR method first evaluates and verifies on the base of 3 key factors. So it reduces the performance of DOS attack in OLSR protocol. In further Research this method can be employed to avoid the DDOS attack Black Whole attack.

REFERENCES

[1] D. Dhillon, J. Zhu, J. Richards, and T. Randhawa, "Implementation & evaluation of an ids to safeguard olsr integrity in manets," in Proceedings of the 2006 International Conference on Wireless Communications and Mobile Computing, ser. IWCMC '06. New York, NY, USA: ACM, 2006, pp. 45–50.

[2] D. Raffo, C. Adjih, T. Clausen, and P. Mühlethaler, "An advanced signature system for olsr," in Proceedings of the 2Nd ACM Workshop on Security of Ad Hoc and Sensor Networks, ser. SASN '04.New York, NY, USA: ACM, 2004, pp. 10–16.

[3] C. Adjih, D. Raffo, and P. Mühlethaler, "Attacks against olsr: Distributed key management for security," in 2nd OLSR Interop/Workshop, Palaiseau, France, 2005. [14] B. Kannhavong, H. Nakayama, and A. Jamalipour, "Nis01-2: A collusion attack against olsr-based mobile ad hoc networks," in Global Telecommunications Conference, 2006. GLOBECOM '06. IEEE, Nov 2006, pp. 1–5.

[4] B. Kannhavong, H. Nakayama, N. Kato, Y. Nemoto, and A. Jamalipour, "Analysis of the node isolation attack against olsr-based mobile ad hoc networks," in Computer Networks, 2006 International Symposium on, 2006, pp. 30–35.

[5] M. Wang, L. Lamont, P. Mason, and M. Gorlatova, "An effective intrusion detection approach for olsr manet protocol," in Secure NetworkProtocols, 2005. (NPSec). 1st IEEE ICNP Workshop on, Nov 2005, pp.55–60.

[6] D. Dhillon, T. Randhawa, M. Wang, and L. Lamont, "Implementing a fully distributed certificate authority in an olsr manet," in Wireless Communications and Networking Conference, 2004. WCNC. 2004 IEEE,vol. 2, March 2004, pp. 682–688 Vol.2.

[7] A. Adnane, C. Bidan, and R. T. de Sousa Júnior, "Trust-based security for the olsr routing protocol," Computer Communications, vol. 36, no. 10, pp. 1159–1171, 2013.

[8] F. Hong, L. Hong, and C. Fu, "Secure olsr," in AdvancedInformationNetworking and Applications, 2005. AINA 2005. 19th International Conference on, vol. 1, March 2005, pp. 713–718 vol.1.

[9] M. Marimuthu and I. Krishnamurthi, "Enhanced olsr for defense against dos attack in ad hoc networks," Communications and Networks, Journal of, vol. 15, no. 1, pp. 31–37, Feb 2013.

[10] Y. Jeon, T.-H. Kim, Y. Kim, and J. Kim, "Lt-olsr: Attack-tolerant olsr against link spoofing," in Proceedings of the 2012 IEEE 37th Conference on Local Computer Networks (LCN 2012), ser. LCN '12. Washington, DC, USA: IEEE Computer Society, 2012, pp. 216–219.

[11] D. Malik, K. Mahajan, and M. Rizvi, "Security for node isolation attack on olsr by modifying mpr selection process," in Networks Soft Computing (ICNSC), 2014 First International Conference on, Aug 2014,pp. 102–106.