Secure MANET'S from DOS Attack using EOLSR

Prof.Masrath Begum
Computer Science and Engineering
Guru Nanak Dev Engineering College, Bidar
State: Karnataka, India

Nitesh.S.P
Computer Science and Engineering
Guru Nanak Dev Engineering College, Bidar
State: Karnataka, India

Abstract: Mobile Ad Hoc Networks (MANETs) form a class of dynamic multi-hop networks consisting of a set of mobile nodes that intercommunicate on shared wireless channels. A MANET node can move freely within network communication range, and server as a router and host which can forward data packets to other hosts according to configured routing protocol. MANETs are self-organizing and self configuring multi-hop wireless networks, where the network structure changes dynamically due to the node mobility. There exists no fixed topology due to the mobility of nodes, interference, multipath propagation and path loss. In this paper we analyze the vulnerabilities of a pro-active routing protocol called optimized link state routing (OLSR) against a specific type of denial-of-service (DOS) attack called node isolation attack. Analyzing the attack, we propose a mechanism called enhanced OLSR (EOLSR) protocol which is a trust based technique to se-cure the OLSR nodes against the attack. Our technique is capable of finding whether a node is advertising correct topology information or not by verifying its Hello packets, thus detecting node isolation attacks. The experiment results show that our protocol is able to achieve routing security with 38% increase in packet delivery ratio and 39% reduction in packet loss rate when compared to standard OLSR under node isolation attack. Our technique is light weight because it doesn't involve high computational complexity for securing the networks.

Keywords: MANET, Optimized link state routing (OLSR), Denial-of –service (DOS), Routing attack.

1. INTRODUCTION

With the advent of mobile computing devices and advances in wireless communication technologies, Mobile Ad Hoc Network has been attracting significant attention from the networking research community. A mobile ad hoc networks (MANET) is a collection of mo-bile devices which are connected by wireless links without the use of any fixed infrastructures or centralized access points. In MANET, each node acts not only as a host but also as a router to forward messages for other nodes that are not within the same direct wireless transmission range. The nodes are free to move and form an arbitrary topology. In addition to freedom of mobility, a MANET can be constructed quickly at low cost, as it does not rely on existing network infrastructure. Due to this flexibility, a MANET is attractive for applications such as emergency operation, disaster recovery, maritime communication, military operation, one-off meeting network, vehicle to vehicle network, sensor network and so on. MANETs are much more vulnerable and are susceptible to various kinds of security attacks [1] because of its cooperating environment. In the absence of a fixed infrastructure that establishes a line of defense by identifying and isolating non-trusted nodes, it is possible that the control messages generated by the routing protocols are corrupted or compromised thus affecting the performance of the network. Routing protocols in MANET can be classified into two categories: reactive protocol and proactive protocol. In proactive routing protocols, all nodes need to maintain a consistent view of the network topology. When a network topology changes, respective updates must be propagated throughout the network to notify the change. In reactive routing protocols for mobile ad hoc networks, which are also called "on-demand" routing protocols, routing paths are searched for, when needed.

Issues of OLSR which is a proactive routing protocol [2] are that it needs more bandwidth and energy resources, overhead, no support for security. Since the MANET assumes a trusted environment, security is major issue. OLSR does not specify any special security measures. As a result OLSR is exposed to various kinds of attacks [3], [4] such as flooding attack, link withholding attack, replay attack, DOS attack and colluding misrealy attack. In this paper, we analyze a specific DOS attack called node isolation attack [5] and propose a solution for it. We propose a solution called enhanced OLSR (EOLSR) that is based on verifying the hello packets coming from the node before selecting it as a multipoint relay (MPR) node for forwarding packets.

ISSN: 2278 – 7798

2. OLSR OVERVIEW

The Optimized Links State Routing (OLSR) [2], [5] is a table driven, proactive routing protocol developed for MANETs. It is an optimization of pure links state protocols in that it reduce the size of control packet as well as the number of control packets transmission required .OLSR reduces the control traffic over head by using Multipoint Relays(MPR),which is the key idea behind OLSR to pro-vide efficient flooding mechanism by reducing the number of transmissions required. Each node selects a set of its neighbor nodes as MPR. Only nodes selected as MPR nodes are responsible for advertising as well as forwarding topology information into the network. OLSR is well suited to large and dense mobile network. Because of the use of MPRs, the large and more dense a network, the more optimized link state routing is achieved. MPRs help providing the shortest path to the destination. The only requirement is that all MPRs declare the links information for their MPR selectors (i.e., the node who has chosen them as MPRs). The network topology information is maintained by periodically exchange link state information .if more reactivity to topological changes is required, the time interval for exchanging of links state information can be reduce. Fig. 2 (A) illustrates a node broadcast its messages throughout the network using standard flooding where all neighbors relay message transmitted by the leftmost node and Fig 2 (B) MPR flooding where only MPR nodes relay the message. A node selects MPRs from among its one hop neighbor with “symmetric”. i.e., bidirectional Linkages. Therefore, selecting the route through MPRs automatically avoids the problems associated with data packet transfer over unidirectional links. In OLSR protocol two types of routing message are used, namely, HELLO message and TC message. A HELLO message is the message that is used for neighbor sensing and MPR selection in OLSR, each node generate HELLO message periodically (every HELLO INTERVAL). A node’s HELLO message contains owns address and the list its 1-hop neighbors. A TC message contains the list of the sender’s MPR selector. The protocol functioning of OLSR is

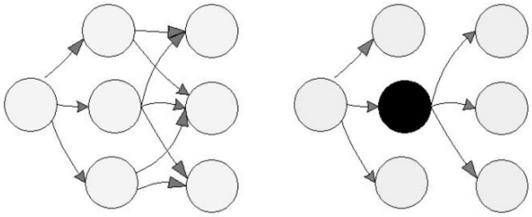

Fig 2 (A) Regular flooding **(b)** MPR flooding

2.1. Neighbor sensing

For neighbor sensing, the HELLO message are broadcasted periodically. The HELLO messages are broadcast only one hop away and are not forward further. These messages are used to obtain the information about neighbors. A HELLO message performs the task of neighbor sensing and MPR selection process. A node’s HELLO message contains its own address, a list of its 1-hop neighbors and a list of its MPR set. Therefore, by exchanging HELLO messages, each node is able to obtain the information about its 1-hop and 2-hop neighbors and can find out which node has chosen it as an MPR.

2.2. MPR flooding

MPR Flooding is the process whereby each router is able to, efficiently, conduct network-wide broadcasts [3], [5]. Each router designates, from among its bi-directional neighbors, a subset (MPR set) such that a message transmitted by the router and relayed by the MPR set is received by all its 2-hop neighbors. Nodes may express, in their HELO messages, their “willingness” to be selected as MPR, which is taken into consideration for the MPR calculation. Each node selects its MPR set from among its 1-hop neighbors such that they can reach all its 2-hop neighbors. The set of router having selected a given router as MPR is the MPR selector -set of that router.

2.3. Link state Advertisement

Link state advertisement is the process whereby nodes are determining which link state information to advertise through the network [3]. Each node must advertise, at least, all links between itself and its MPR-selector-set, in order to allow all nodes to calculate shortest paths. Such link state advertisements are carried in TCs, broadcast through the network using the MPR flooding process. As a node selects MPRs only from among its bi-directional neighbors, links advertised in TC are also bi-directional and routing paths calculated by OLSR contain only bi-directional links. TCs are sent periodically, however certain events may trigger non-periodic TCs.

3. NODE ISOLATED ATTACK

Here we present a node isolated attacks which can results in denial-of-service against OLSR protocol

[5]. The goal of this attack is to isolated a node from communicating with other node in the network more specifically this attack prevent the victim node from receiving data packets from other node in to the networks. The idea of this attack is that attackers prevent link information of a specific node, the group of nodes. From being spread to the whole network. Those other node who could not receive the link information of the target node will not be able to build a route to the target node and hence will not able to send data to these nodes.

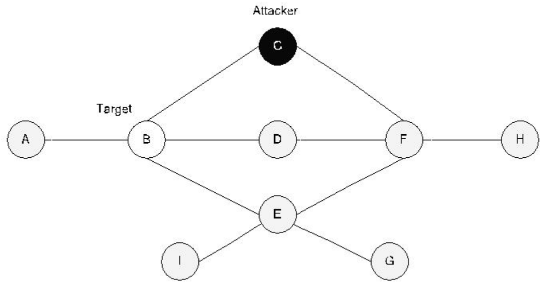

Fig 3.1 node isolation attack (A) Topology perceived by Node **H** before the attack

In this attack, attackers create a virtual link by sending fake HELLO message including the address list of target nodes 2-hop neighbors. (The attacker can learn its 2-hop neighbors by analyzing the TC message of its 1-hop neighbors.) According to the protocol, the target node will select attacker to be its only MPR. Thus the only node that must forward and generate TC message from the target node is the attacking node. By drooping TC message received from the target node and not generating the TC message for the target node, the attacker can prevent the link information of the target node for being disseminated to the whole network. As a result, other node would not be able to receive link information of a target node will conclude that a target node doesn't exist in the network. Therefore, a target node's address will be removed from the other node's routing tables. Since in OLSR, through HELLO message each node can obtain only information about its 1-hop and 2-hop neighbors, other node that are more than 2-hopes away from the target node will not be able to detect the existence of the target node. As a consequence, the target node will be completely prevented from receiving data packets from nodes that are three or more hops away from it.

In Fig. 3.1(A), node C is the attacking node, and node B is the tar-get node. Instead of sending correct HELLO message that contain {B, F} in neighbor address list, the attacker sends a fake HELLO message that contains {B, F, G, Z} which includes the target node's all 2-hop neighbors {F, G}and one non-existent node {Z} [5]. According to the protocol, the target node B will select the attacker C as it's only MPR. Here node Z is announced only by the attacker and not by any other neighbor nodes of the victim. This is to improve the possibility of attacker being selected as a MPR. So the victim node B assumes that its 2- hop neighbor node Z can be reached only via node C (attacker) and all the other 2-hop neighbors also can be reached through node C itself. So it selects node C as it's only MPR. Being node B's only MPR, the

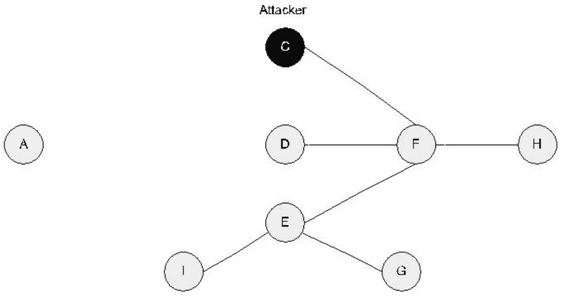

Fig 3.1(B) Topology perceived by Node **h** after the attack.

Attacker refuses to forward and generate TC message for node B. Since the link information of node B is not propagated to the entire network, other nodes whose distance to node B is more than two hops (e.g., node H) would not be able to build route to node B. Fig. 3.1(B) shows the topology perceive by node H after the node isolation attack [5]. As a result, other nodes would not be able to send data to node B. Despite being in the network, the target node B will be isolated from the network. An attacker can launch this attack, as long as the target node is within its transmission range.

4. RELATED WORK

Most of the previous works on security attacks have mainly addressed in reactive routing protocol such as AODV and DSR protocol. In [10], Ning and sun analyzed in detail and evaluated several possible insider attacks against the AODV protocol including route disruption and resource consumption attack. Several cryptographic based techniques had been Contributed for securing OLSR [6]-[9].

In [11], Hu et al. introduced a rushing attack which results in Dos attacks on MANET. The same authors also presented a wormhole attack as well as the counter measure against the attack [12]. Wang et al. [13] studied and showed that false distance vector and false destination sequence attacks can lead to decrease of up to 75% in data delivery ratio. In [14][15] , the influence of resource consumption attack on the performance of AODV protocol has been studied. Kurosawa et al. [16] presented an analysis of black hole attack on AODV protocol. In [17], a passive attack model against AODV protocol has been proposed.

[7],[8],[5],[18] a number of articles has analyzed security properties and vulnerabilities of routing protocols in MANETs() these papers identify resources of MANET routing protocol that are potentially vulnerable to attacks, and propose several attacks against these resources, as well as counter-measures against such attacks.

In [5] and [11], the authors proposed a simple mechanism to detect the link withholding and misrelay launched by MPR nodes based on overhearing of traffic generated by 1-hop neighbors. But this technique requires promiscuous listening of neighbor nodes which result in energy drop at this node whereas we do not use any neighbor monitoring approach.

A formal approach to handle the MPR selection and defense against the security attacks in OLSR is suggested in [13]. This approach validates the routing table and the topology information using trust based reasoning. Hence, each node can verify the validity of the received HELLO and TC messages simply by correlating the information provided by these messages.

5. PROPOSED WORK

In previous work node isolated attack is avoided using two phase mechanism. We propose a solution using trust analysis to verify whether corresponding node is malicious or not. Trust based analysis is derived from idea mentioned in [3]. Our method uses HOP_INFORMATION table, 2- hop request and 2-hop reply. Generally, OLSR nodes trust all information that received from its 1-hop neighbor. Here we analyze the pattern of Hello message of the node that advertise all 2-hop neighbors as its 1-hop neighbors and verify whether that node is malicious or not. In OLSR, TC and HELLO message are used to select MPR and route calculation. Each node must broadcast periodically HELLO message to indicate its existence. In this mechanism, each node maintains HOP_INFORMATION table which contains of HELLO message sender and its 2-hop neighbors. In Fig 5.1 A selects B, C and D as MPR to broadcast packets to T,U,V and maintains HOP_INFORMATION table show in Table 5.1

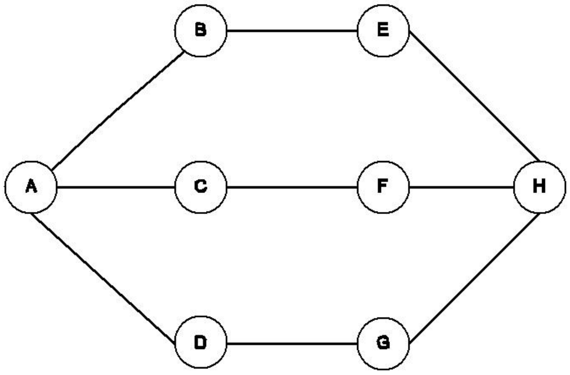

Fig. 5.1 OLSR node A selects B, C, and D as MPR.

HELLO message sender	2-hop neighbors
B	E
C	F
D	G

Table 5.1 P's HOP_INFORMATION

In Fig. 5.2, if new node X sends HELLO message as shown in Table 5.2 advertising all the target node's 2-hop neighbors as its 1-hop neighbors along with a new neighbor Z. then A add X's 1-hop information in A's HOP_INFORMATION table as show in Table 5.3

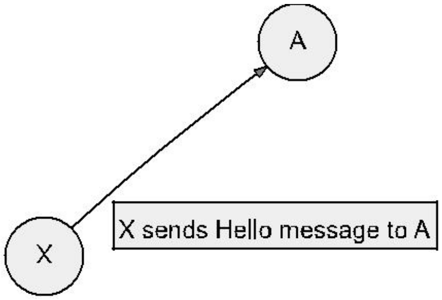

Fig. 5.2 X advertises its neighbor nodes to A.

Originator	Neighbors
X	E,F,G,Z

Table 5.2. X's neighbors.

After including X's information, (Fig 5.3) A send 2-hop request to its 1-hop neighbors B,C,D and then the node B,C and D forward2-hop request to their 1-hop neighbor E,F,G to verify whether node X in its HOP_INFORMATION table.

HELLO message sender	2-hop neighbors
B	E
C	F
D	G
X	E,F,G,Z

Table 5.3. A's ONE_HOP table after receiving X's HELLO message

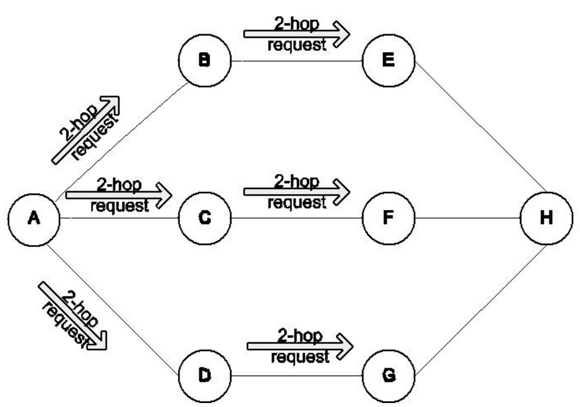

Fig.5.3. A send 2-hop request to B, C, and D then B, C, and D send request to E, F, and G.

If node X founds in the table, (Fig 5.4) then E,F,G sends 2-hop reply to A through B,C,D indicating X is its 1-hop neighbor. If so, A will select X as a MPR and broadcast through X to H. otherwise A add X in Blacklist and discard its HELLO message.

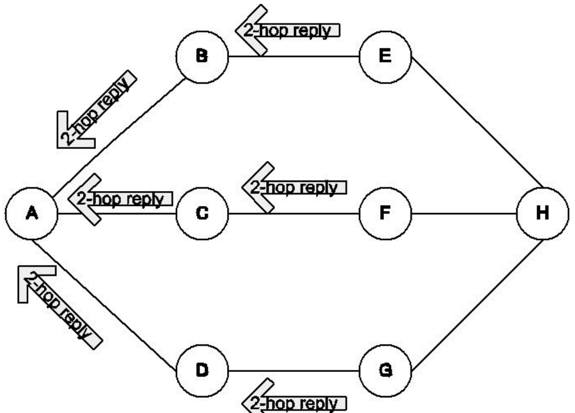

Fig. 5.4 E, F, and G send 2-hop reply to A through B, C, and D.

Node A then informs about the presence of malicious node X to the network through HELLO and TC messages. The nodes on receiving the malicious node information then delete the entire route involving that node from their routing table. It also ignores all the HELLO and TC message coming from that node. In other case, if node X is actually be in the coverage area of E,F,G nodes, then the target node A queries about the existence of node Z in the networks through the NEQ message forwarded through its current MPR nodes. If any designated MPR node in the network confirms the existence of node Z, then node X will be selected as MPR, otherwise, it will be confirmed as a malicious node. Moreover, colluding attacks are not possible because our technique doesn't employ any neighbor node monitoring except explicit verification of the Hello messages it receives. The processing takes place at each node after receiving a Hello packet is described in Algorithm 1. Algorithm 2 depicts the behavior of a node after receiving a 2-hop request. Due to congestion in the network or node mobility, if any of the two-hop replay is lost, the sores node after a time out period resend the 2- hop request packet to the corresponding node from which the replay is not received. Only if 2-hop replay is received from all the 2-hop neighbors, and after verifying the trustworthiness of the node in question, it will be selected as the new MPR node. Otherwise, data forwarding will be continued using the exiting MPR nodes only.

Algorithm 1 HELLO reception.

```
if originator_node not in malicious list then
    Add the hello packet information in ONE_HOP table
    if 2-hop reply received then
        Verify the proof of correctness advertised by the
        hello packet sender node
        if correct then
            Select that node as its MPR if required
        else
            Move the hello packet sender to malicious list
        end if
    end if
    Inform the network about the presence of the attacker
end if
```

Algorithm 2 2-Hop request reception.

```
if 2-hop request received then
    Send a 2-hop reply containing all its one hop neighbors
    information
end if
```

6. SIMULATION MODEL AND RESULTS

In our strategy rate adjustment at any node in the network does not depend only on the immediate next hop but also the nodes that are more than one hop away on the way to the sink. Thus, the value of congestion factor that is propagated is cumulative and reflects the state of congestion at nodes upstream. Another thing to be taken into account is that we do not want the suppress message to be sent when there is no congestion in this part of the network. Hence, the congestion factor is propagated, in other words, the suppress message is sent only when there is congestion. It is not propagated beyond the region where there is no congestion. The scheme approximates to closed loop in case of persistent congestion.

A node calculates its congestion factor based on the factors described above. Then it compares this value to a threshold and if this value is greater than this threshold value, it sends a suppress message downstream. Note that if this node receives a suppress message and reduces its rate, its queue lengths would start increasing and hence, it may cause a suppress message to be sent further.

6.1 Modules

A. Network Topology Creation

Create a base Wireless Sensor network topology with more number of nodes for "organizing Bluetooth security" and transfer the data from source to Destination.

B. Routing Protocol Deployment

Create a Bluetooth adhoc network topology with more number of nodes and implement Existing Protocol, the major problems in heterogeneous wireless sensor network are interference and congestion, which minimize quality data transmission.

C. Secure Protocol Creation

Create a network topology with more number of nodes and implement security protocol to increase the quality in data transmission in Bluetooth adhoc network by implementing key management technique and security techniques and transmit the packets from source to destination.

D. Performance Evolution

In this section, we present the performance evaluation on our technique using extensive simulations conducted with the network simulator 2 [19]. The default settings as in the specifications of OLSR [2] were used for HELLO and TC messages. In our simulation, we used 31% of malicious nodes out of the normal nodes to launch the attack. The malicious nodes are chosen randomly and also one of the neighbors of the nodes that are generating the data traffic is chosen as malicious nodes. The traffic load is simulated using 15 user datagram protocol-case based reasoning (UDP-CBR) connections generating traffic of 5 kB UDP packets (data payload 512 Bytes) with an inter departure time of 1 s. To eliminate the randomness in the result, for each metric, simulation is done for ten different seed values with different random movement of nodes and the average value is taken for the result.

We used the following metrics to evaluate the performance of our proposed solution EOLSR against OLSR under attack and the results obtained are shown in Figs. 8–10.

1. Packet delivery ratio: The ratio between the number of packets originated by the CBR sources of source nodes and the number of packets received by the CBR sink at the destination node.
2. Packet loss rate: It is the number of data packets dropped by the malicious nodes that are selected as MPR nodes.
3. Control packet overhead: This is the ratio of number of control packets generated to the data packet received.

Fig. 8 shows the packet delivery ratio in the presence of node isolation attack. Here 1 to 5 malicious nodes are randomly selected to launch the attack. They select any one of the neighbor nodes as their victim and after analyzing the TC messages and hello messages coming from that node; they create a fake hello message containing all the 2-hop neighbors of the victim and send it to the victim. Once the victim selects it as its MPR, they drop all the data packets and TC packets coming from the victim. As shown in the figure, The throughput achieved by OLSR was approximately 25%, while the throughput achieved in EOLSR under the same scenario was approximately 63%, in-creased by 38% i.e., EOLSR improved the throughput achieved by OLSR under attack. When the number of attackers increases, the throughput nearly drops to zero in normal OLSR whereas in our scheme, even though the number of attackers increases, the throughput achieved is more or less in steady state because the MPR selection is made only after verifying the correctness and trustworthiness of the node. Similarly, the throughput achieved by the existing approach [5] is 65% which is 5% less than our scheme. This is because the existing solution in [5] does not verify the trustworthiness of a node before selecting it as an MPR. Instead after selecting the MPR node, it overhears the packet forwarded by that MPR node and compares it with the packets send by itself to verify whether the MPR node is forwarding the packets or not. Since the detection of malicious MPR node is possible after the dropping of some TC and data packets by the MPR node, the throughput achieved in [5] is lesser than our scheme.

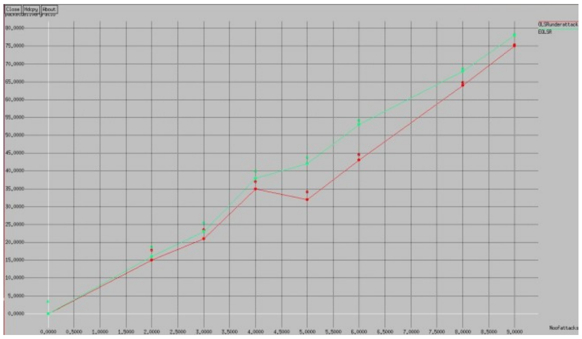

Fig 8. Packet Delivery ratio

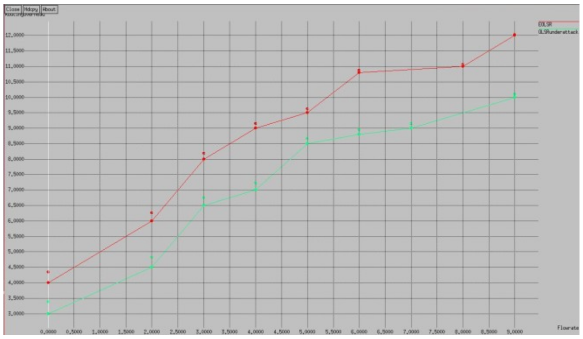

Fig 9. Control packet overhead

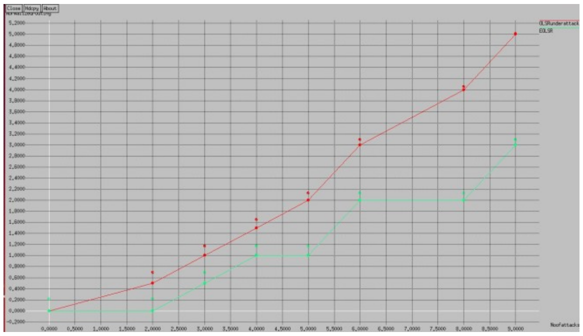

Fig 10. Normalized Routing

Fig.9 shows the number of packets dropped by the malicious nodes in OLSR and EOLSR. The packets loss rate of OLSR under attack was approximately 74%, while the packet loss rate of EOLSR was approximately 35%, reduced by 39%. The control packets ratio of EOLSR is 54% which is 8% higher than the control packet ratio of the solution in [5] which is 46%.This is because of the additional control packets introduced in EOLSR to prevent the node isolation attack by verifying MPR nodes.

7. CONCLUSION

This paper proposes a solution for node isolation attack launched against OLSR routing protocol. Here, we have discussed through an attack model, that it is easy for a malicious node to launch the node isolation attack to isolate an OLSR MANET node. This attack allows at least one attacker to pre-vent a specific node from receiving data packets from other nodes that are more than two hops away. The proposed solution called EOLSR, which is based on OLSR, uses a simple verification scheme of hello packets coming from neighbor nodes to detect the malicious nodes in the network. The experiment results show that the percentage of packets received through our proposed work is better than OLSR in presence of multiple attacker nodes. The simulation is done using Network Simulator 2 [19] and our scheme is found to achieve routing security with 38% increase in packet delivery ratio than standard OLSR and also achieves 39% reduction in packet loss rate than OLSR. Compared to other related works, the proposed protocol has more merits; the most important merit is that it achieves degradation in packet loss rate without any computational complexity or promiscuous listening. Moreover, cooperative or colluding attack cannot be launched, because our technique doesn’t employ any promiscuous listening of neighbor nodes for detecting the attackers.

REFERENCES

[1] B. Kannhavong, H. Nakayama, and A. Jamalipour, "A survey of routing attacks in mobile ad hoc networks," *IEEE trans. Wireless Commun.*, vol. 14, no. 5, pp. 85–91, Oct. 2007.

[2] T. Clausen and P. Jacquet, "IETF RFC3626: Optimized link state routing protocol (OLSR)," *Experimental*, 2003.

[3] T. Clausen and U.Herberg, "Security issues in the Optimized link state routing protocol version 2 (OLSRv2)," *Int. J. Netw. Security Appl.*, 2010.

[4] B. Kannhavong, H. Nakayama and A. Jamalipour, "A study of routing attack in OLSR-based mobile ad hoc networks," *Int. J. Commun. Syst.*, 2007.

[5] B. Kannhavong, H. Nakayama, N. Kato, Y. Nemoto, and A. Jamalipour, "Analysis of the node isolation attack against OLSR-based mobile ad hoc network," in *Proc. ISCN*, 2006, pp. 30–35.

[6] D. Raffo, C. Adjih, T. Clausen, and P. Muhlethaler, "Securing the OLSR protocol," in *Proc. Med-Hoc-Net*, 2003.

[7] D. Raffo, C. Adjih, T. Clausen, and P. Muhlethaler, "An advanced signa-ture system for OLSR," in *Proc. ACM SASN*, 2004.

[8] D. Raffo, C. Adjih, T. Clausen, and P. Muhlethaler, "Attacks against OLSR: Distributed key management for security," in *Proc. OLSR Interop and Workshop*, 2005.

[9] C. Adjih, T. Clausen, A. Laouiti, P. Muhlethaler, and D. Raffo, "Securing the OLSR routing protocol with or without compromised nodes in the network," HIPERCOM Project, INRIA Rocquencourt, Tech. Rep. INRIA RR-5494, Feb. 2005.

[10] Ning P, Sun K. "How to misuse AODV: a case study of insider attacks against mobile ad-hoc routing protocols". Technical Report TR-2003-07, North Carolina State University, Department of Computer Science, 2003.

[11] Hu Y-C, Perrig A, Johnson D. "Rushing attacks and defense in wireless ad hoc network routing protocols". ACM Workshop on Wireless Security (WiSe 2003), San Diego, California, U.S.A., 19 September 2003.

[12] A. J. P. Vilela and J. Barros, "A cooperative security scheme for optimized link state routing in mobile ad-hoc networks," in *Proc. IST MWCS*, 2006.

[13] Wang BBW, Lu Y. "On vulnerability and protection of ad hoc ondemand distance vector protocol". International Conference on Telecommunication, France, Paris, 2003.

[14] X. Zeng, R. Bagrodia, and M. Gerla, "GloMoSim: A library for parallel simulation of large-scale wireless networks," in *Proc. PADS*, 1998.

[15] D. Raffo, "Security schemes fo the OLSR protocol for ad hoc networks," Ph.D. dissertation, Univ. Paris, 2005.

[16] Kurosawa S, Nakayama H, Kato N, Nemoto Y, Jamalipour A."Detecting blackhole attack on AODV-based mobile ad hoc networks by dynamic learning method". International Journal of Network Security 2007, in press.

[17] Hong X, Kong J, Gerla M. "A new set of passive routing attacks in mobile ad hoc networks". Proceedings of IEEE Military Communications Conference (MILCOM'03), Boston, MA, 13–16 October 2003.

[18] T. Clausen, U.Herberg, "Security Issues in the Optimized Link State Routing Protocol Version 2 (OLSRv2)", International Journal of Network Security and its Applications, 2010.

[19] "The Network Simulator - ns-2," http://nsnam.isi.edu/nsnam/ index.php/User Information, 2012.