ISSN:0975-9646

Enhanced OLSR for Defense against Node Isolation Attack in Ad Hoc Networks

Banoth Balaji , Mohammed HasanKhan , R. Prathap Kumar

Computer Science and Engineering
Vignan University
Guntur, AP, India.

***Abstract*: A Mobile Ad Hoc Network is constructed by a set of self-configured mobile nodes that are connected by wireless links without infrastructure. 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. In MANETs, applications are mostly involved with sensitive and secret information. Since MANET assumes a trusted environment for routing, security is a major issue. In this paper we analyze the vulnerabilities of a pro-active routing protocol called OLSR (Optimized link state routing) 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 trust based technique to secure 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.**

***Keywords*: - MANET, Optimized link state routing (OLSR), Denial-of –service (DOS), Node isolation attack, 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 Network (MANET) is a collection of mobile nodes interconnected by wireless links without the aid of any fixed infrastructure or centralized access point. In MANET, each node act both as a host and as a router to forward messages for other nodes that are not within the same radio 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. Routing protocol in MANET can be classified in two categories: reactive protocol and proactive protocol. In proactive routing protocol, 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 changes. Reactive routing protocols for mobile ad hoc network are also called "on-demand" routing protocol. In a reactive routing protocol, routing paths are searched for when needed. Issues of OLSR 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 such as flooding attack, link withholding attack, replay attack, DOS attack and colluding misrealy attack. In this paper we analyze the specific Dos attack called node isolation attack and propose a solution for it.

2. OLSR OVERVIEW

The Optimized Links State Routing (OLSR) 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.A MPR is a node's one-hop neighbor which has been chosen to forward packet. Instead of pure flooding of the network, packets are just forwarded by a node's MPRs; this delimits the network over head, thus being more efficient than pure link state routing protocols. 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. Figure 2 (a) illustrates a node broadcast its messages throughout the network using regular flooding and figure 2 (b) broadcasting using MPR.

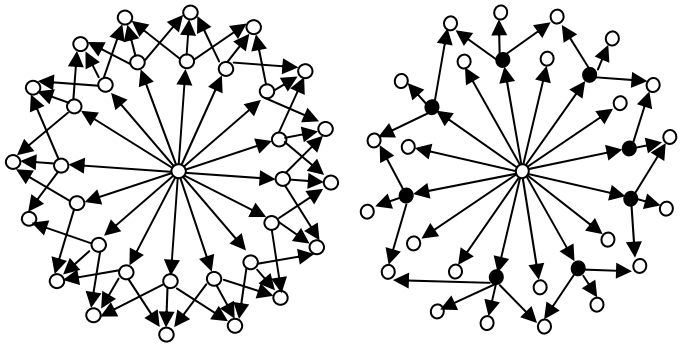

Figure 2 (a) Regular flooding **(b)** MPR flooding

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 uni-directional 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

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 broadcast. 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. MPR selection is encoded in outgoing HELLOs. Router may express, in their HELLO message, their "willingness" to be selected as MPR, which is taken in to consideration for the MPR calculation, and which is use full for example when an OLSR network is "planned". 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 routers are determining which link state information to advertise through the network. Each router must advertise, at least, all the links between itself and its MPR selector- set, in order to allow all routes to calculate shortest paths. Such link state advertisements are carried in TCs, broadcast through the network using the MPR flooding process described above. As a router selects MPRs only from among bi-directional neighbors, links advertised in TC are also bi-direction and routing paths calculated by OLSR contains 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. 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.

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.

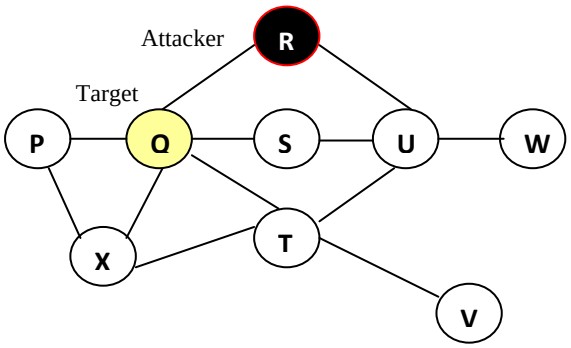

Figure 3.1 node isolation attack (a) Topology perceived by Node **W** before the attack

In figure 3.1(a) Node R is attacking node, and Node Q is target node. Instead of sending correct HELLO message {Q,U} in neighbors address list the attacker send a fake Hello message that contains{Q,U,V,A} which include the target nodes all 2-hop neighbors {U,V} and one non existing node {A}. According to the protocol, the target Node Q will select the attacker R as it's only MPR being Node Q's the only MPR, the attacker refuse to forward and generate a TC message for Node Q. since the link information of the Node Q is not propagated to the entire network. Other nodes whose distance to Node Q is more than two hopes (e.g. Node W) would not be able to build route to Node Q. as a result, other node would not be able

to send data to Node Q. despite being in the network, and the target Node Q will be isolated from the network. An attacker can launch this attack, as long as the target node is within its transmission range.

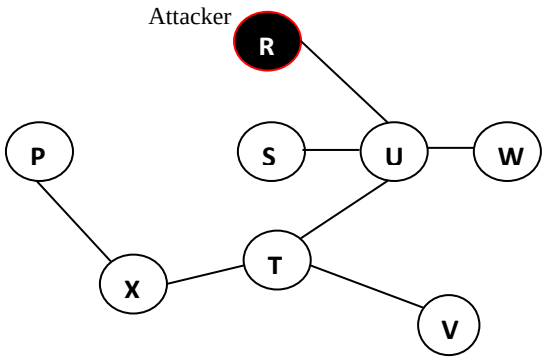

Figure 3.1(b) Topology perceived by Node **W** after the attack.

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.

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.

[2] Proposed a distributed CA to authenticate nodes to prevent identity spoofing attack.

[4] Proposed Cryptography solution which uses timestamp and asymmetric key to guard control packets to avoid replay attacks.

[6] Present a more detailed security analysis of the OLSR routing protocol and analyze the DOS attack and present a simple technique to detect and avoid the attack.

[9] Proposed an intrusion detection technique that observed TC messages from its MPR node regularly to detect Malicious MPR nodes.

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 figure 5.1 P selects Q,R and S as MPR to broadcast packets to T,U,V and maintains HOP_INFORMATION table show in table 5.1

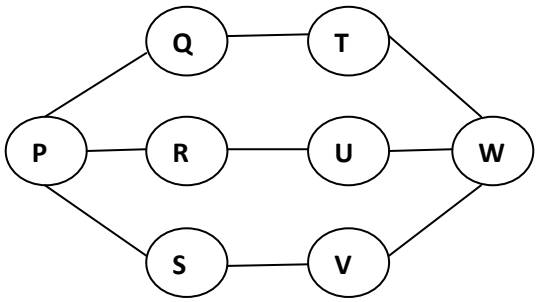

Figure 5.1 OLSR nodes, P selects Q,R,S as MPR.

Table 5.1 P's HOP_INFORMATION

HELLO message sender	2-hop neighbors
Q	T
R	U
S	V

In figure 5.2, if new node Y 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 A. then P add Y's 1-hop information in P's HOP_INFORMATION table as show in table 5.3.

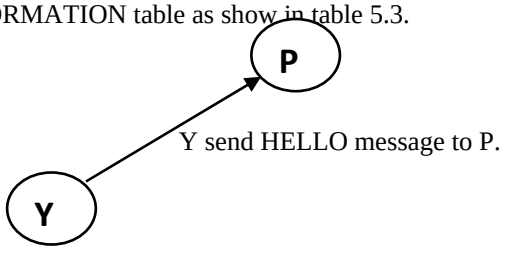

Figure 5.2 Y advertise its neighbor to P

Table 5.2 Y's HELLO message

Originator	Neighbors
Y	T,U,V,A

Table 5.3 P's HOP_INFORMATION table after receiving Y's HELLO message

HELLO message sender	2-hop neighbors
Q	T
R	U
S	V
Y	T,U,V,A

After including Y's information, (figure 5.3) A send 2-hop request to its 1-hop neighbors Q,R,S and then the node Q,R and S forward2-hop request to their 1-hop neighbor T,U,V to verify whether node Y in its HOP_INFORMATION table.

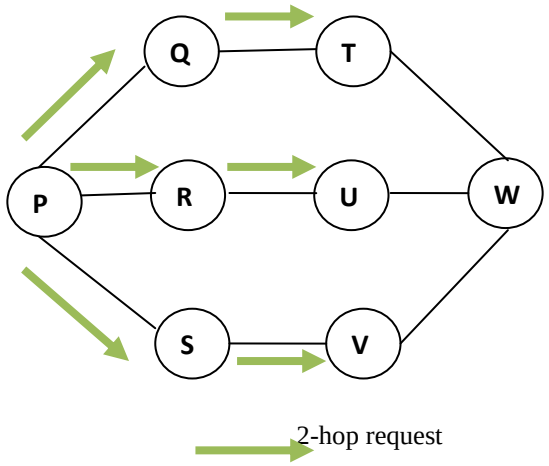

Figure 5.4 P send 2-hop request to Q,R,S then Q,R,S send request to T,U,V.

If node Y founds in the table, then T,U,V sends 2-hop reply to P through Q,R,S indicating Y is its 1-hop neighbor. If so, P will select Y as a MPR and broadcast through Y to W. otherwise P add Y in Blacklist and discard its HELLO message.

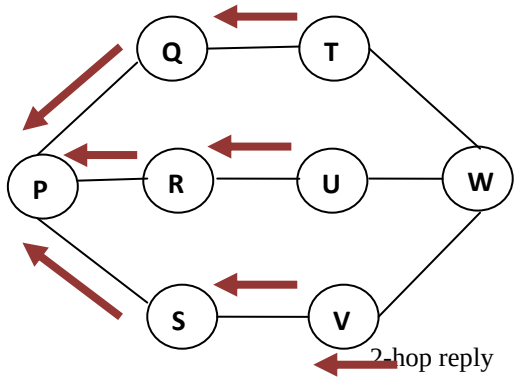

Figure 5.4 T,U,V send 2-hop reply to P through Q,R,S.

Node P then informs about the presence of malicious node Y 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 Y is actually be in the coverage area of T,U,V nodes, then the target node P queries about the existence of node A 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 A, then node Y 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.

1. **If** originator_node not in malicious list **then**
2. Add the hello packet information in ONE_HOP table
3. **If** 2-hop reply received **then**
4. Verify the proof of correctness advertised by the
5. Hello packet sender node
6. **If** correct **then**
7. Select that node as its MPR if required
8. **Else**
9. Move the hello packet sender to malicious list
10. **End if**
11. **End if**
12. Inform the network about the presence of the attacker
13. **End if**

Algorithm 2 2-Hop request reception

1. **if** 2-hop request received **then**
2. Send a 2-hop reply containing all its one hop neighbors
3. Information
4. **End if**

6. Simulation Model And Results

In this section, we present the performance evaluation on our technique using simulation conduct with the network simulator GLOMOSIM [20]. We generated random topology with a maximum of 50 nodes over a rectangle field. The terrain dimension is fixed as 750*1000m. the maximum transmission range of each node is 250m. the duration of the simulation is 600s. Random way point model is used as the mobility model for each node. Node speed is varied from 2m/s to 25m/s. the node pause time is

varied from 0 seconds to 300 seconds. The default setting as in the specification of OLSR were used for HEELLO and TC message. In our simulation, we used 35% 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 node that are generating the data traffic is chosen as malicious nodes. Te traffic load is simulated using 15 user datagram protocol-case based reasoning (UDP-CBR) connections (30 nodes) generating traffic of 5KB UDP packets (data payload 512 bytes) with in 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 taken for the result. Also our approach is compared is with another existing approach [19].

Performance Evaluation

We used the following metric to evaluate the performance of our proposed solution EOLSR against OLSR under and the result obtained are show in fig.8-10.

1. Packet deliver ratio: The ratio between the number of packets originated by the CBR source nodes and the number of packets received by the CBR sink at the destination node.
2. Packets 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 packet generated to the data packet received.

Fig.8 show the packet deliver ratio I the presence of node isolation attack. Here 1to5 malicious nodes are randomly selected to launch the attack. They select any one of the neighbor nodes as there victim and after analyzing the TC message and hello message coming from the node; they create a fake hello message contain all the 2-hop neighbor of the victim and send it to the victim. Once the victim selects it as its MPR, they drop all the data packet and TC packet coming from the victim. As shown in the figure, the through put achieved by LOSR was approximately 25%, while the throughput achieved in EOLSR under the same scenario was approximately 70%, increased by 45%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 [19] is 65% which is 5% less than our scheme. This is because the existing solution in [19] 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 packet 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 [19] is lesser than our scheme.

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 30%, reduced by 44%. Similarly the packet loss rate of existing solution in [19] was approximately 37%, which was increased by 7% when compared to our solution. This is because the existing solution [19] is a detection technique, which detects the attack after it has been launched whereas our technique verifies the trustworthiness of a node before selecting it as an MPR so packet drop ratio of our approach is less when compared to the solution in [19]. Moreover, the existing approach in [19] employs promiscuous listening to overhear packets forwarded by the MPR nodes which results in energy dropping at the individual nodes and also this technique cannot withstand colluding attackers. Whereas our technique does not employ promiscuous listening so colluding attacks are not possible and also energy consumption at each node will be much lesser than in [19].

The control packets ratio of EOLSR is 57% which is 11% higher than the control packet ratio of the solution in [19] which is 46%. This is because of the additional control packets introduced in EOLSR to prevent the node isolation attack by verifying MPR nodes.

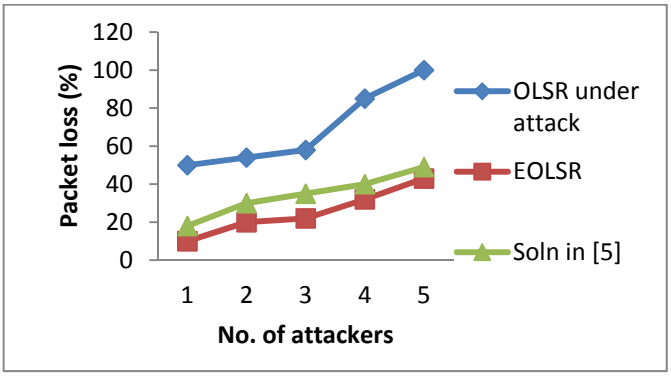

Fig 8. Packet Delivery ratio

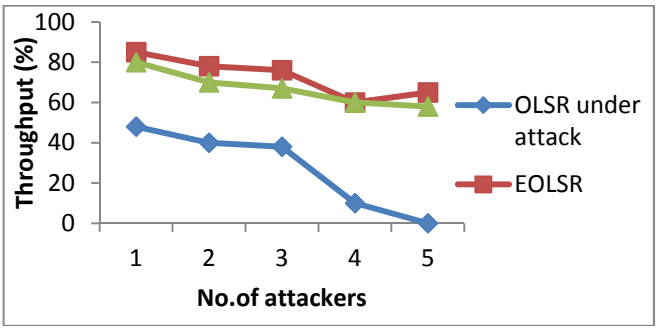

Fig 9. Packet loss ratio

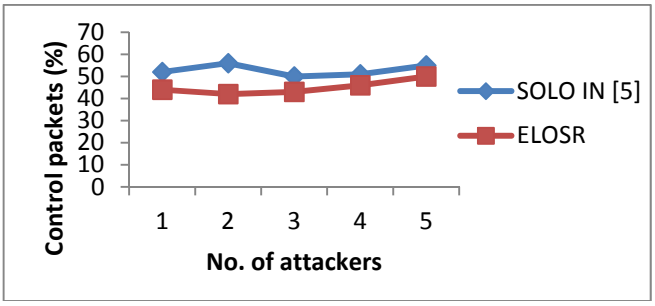

Fig 10. Control packet overhead

7. CONCLUSION

This paper proposes a better solution for a node isolation attack launched on OLSR routing protocol. In this we discussed an attack model, which is easy for malicious node to launch node isolation to isolate an OLSR MANET node. Here the attack allows at least one attacker to prevent a specified node from receiving data packets of other nodes which have more than two hops away. The solution which we have proposed called EOLSR, based on OLSR takes use of simple verification scheme of Hello packets which comes from neighbors nodes to identify malicious node in network. According to experimental results the percentage of packets received by the proposed work has better percentage than OLSR in existence of attacker nodes. Here simulation done with the use of GloMoSim and the schema is found to achieve routing security with an increase of 45% in ratio of packet delivery to that of standard OLSR and gains 44% reduction in packet loss rate than OLSR. The proposed protocol done by us has number of merits when compared to the other related works. In the merits of the proposed protocol the important merit is that it gains degradation in packet loss rate with no computational complexity. Moreover, cooperative or colliding attack could not be launched because the technique which we have implemented doesn't employ promiscuous listening of neighbor nodes for identifying the attackers.

REFERENCE

[1] T. Clausen, P. Jacquet, "RFC3626: Optimized Link State Routing Protocol (OLSR)", Experimental,http://www.ietf.org/rfc/rfc3626.txt

[2] D.Dhillon, T.s Randhawa, "Implementing a Fully distributed Certificate Authority in an OLSR MANET", IEEE WCNC 2004.

[3]. Asmaa Adnane, Rafael Tim´oteo de Sousa Jr, Christophe Bidan, and Ludovic M´e, "Analysis of the implicit trust within the OLSR Protocol" IFIP International Federation for Information Processing, Nov 2007

[4]. Raffo D, Adjih C, Clausen T, Muhlethaler P. "An advanced signature system for OLSR". Proceedings of the 2004 ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN 04), Washington, DC, U.S.A., 25 October 2004.

[5]. B. Kannhavong, H. Nakayama, A. Jamalipour, "A survey of Routing Attacks in Mobile Ad hoc Networks", IEEE Wireless Communications, Oct 2007.

[6]. B. Kannhavong, H. Nakayama, A. Jamalipour, "A study of routing attack in OLSR-based mobile ad hoc networks", International Journal of Commnication Systems 2007, 1241-1261.

[7]. F. Hong, L.Hong, "Secure OLSR", Proceedings of the 19th International Conference on Advanced Information networking and Applications, 2005 IEEE.

[8].D. Raffo, "Securing OLSR Using Node Locations," Proc. 2005 Euro. Wireless, Nicosia, Cyprus, Apr. 10–13, 2005.

[9]. B. Kannhavong., "Analysis of the Node Isolation Attack against OLSR- Based Mobile Ad Hoc Network," 7th International Symposium on Computer Networks, 2006.

[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]. Hu Y-C, Perrig A, Johnson D. "Packet leashes: a defense against wormhole attacks in wireless networks". Proceedings of the 22nd Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM), San Francisco, CA, U.S.A., 2003; 1976–1986.

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

[14]. Yi P, Dai Zh, Zhang Sh, Zhong Y. A new routing attack in mobile ad hoc networks. International Journal of Information Technology 2005; 11(2):83–94.

[15]. Desilva S, Boppana RV. "Mitigating malicious control packet floods in ad hoc networks". Proceedings of IEEE Wireless Communication and Networking Conference, New Orleans, Lucian, U.S.A., 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]. B.Kannhavong, H. Nakayama, N. Kato, Y. Nemoto, and A. Jamalipour, "Analysis of the node isolation attack against OLSR-based mobile ad hoc netwok," in proc. ISCN, 2006, pp. 30-35.

[20]. X. Zeng, R. Bagrodia, and M. Gerla, "GloMoSim: A Library for parallel simulation of large-scale wireless networks," in proc. PADS, 1998.