International Journal of Security and Its Applications
Vol.8, No.5 (2014), pp.51-64
http://dx.doi.org/10.14257/ijsia.2014.8.5.06

A Defense Mechanism for EOLSR against DOS Attacks in Ad hoc Networks Using Trust Based System

Banothu Balaji[1], Mohammed Hassan Khan[1], T.S.N. Murthy[1] and Tai-hoon Kim[2,1]

[1]*Department of Computer Science and Engineering*
Vignan's University, Guntur, AP, India.
{balajiwgl,hasankhan1251,murthyteki}@gmail.com
[2]*Department of Convergence Security,*
Sungshin Women's University,
249-1, Dongseon-dong 3-ga,
Seoul, 136-742, Korea
taihoonn@daum.net

Abstract

The process of routing in MANET (Mobile ad hoc network) requires a trust based environment and therefore security is one of the major concern. A backbone network in a MANET is difficult when it is implemented for a specific application. A security based environment is one of the most critical issues in a MANET because it is mostly involved with sensitive and secret information. This work deals with a specific type of denial-of-service (DOS) attack called node isolation attack and thus analyze the vulnerabilities of a pro-active routing protocol called optimized link state routing (OLSR). Based on this analysis, this work proposes a mechanism called enhanced OLSR (EOLSR) protocol which is a trust based technique to secure the OLSR nodes against the attack. According to the proposed technique, isolation can be detected by the hello packets it sends. Verification is done through this, whether a node is advertising correct topology information or not thus leading to detection of the isolation node that perform the DOS attack. Enhanced OLSR is further improved using the trust based system called Trustbased OLSR (TOLSR). Once the node is detected as attacker using EOLSR, its trust value is reduced to half of its initial value. Hence in future, selection of attacker as MPR node is prevented since all the nodes will select only high trust node as MPR node. The concept of ensuring security to the network does not involve much computational complexity and therefore, the proposed scheme is a light weight technique.

Keywords: *Manet, Optimized link state routing (olsr), Enhanced optimized link state routing (eolsr), Trustbased optimized link state routing (tolsr), Routing attacks*

1. Introduction

Ad-hoc network is one of the emerging trends in wireless communication. In conventional wireless communication there is need of base station for communication between two nodes. These base station leads to more infrastructures and more cost. An ad hoc network facilitates communication between nodes without the existence of an established infrastructure. Nodes

(Corresponding Author)

ISSN: 1738-9976 IJSIA

are connected randomly using ad-hoc networking and routing among the nodes is done by forwarding packets from one to another which is decided dynamically. In general, MANET's are formed dynamically by an autonomous system of mobile nodes that are connected via wireless links without using any centralized administration [1]. Mobile nodes that are within each other's radio range communicate directly via wireless links, while those that are far apart rely on other nodes to relay messages as routers. Node mobility in an ad hoc network causes frequent changes of the network topology.

2. Classification of Routing Protocol

In MANET, each node between source and destination acts as routers. The routing of data packets from source to destination are controlled by different routing protocols. Different routing protocols are classified as shown in Figure.

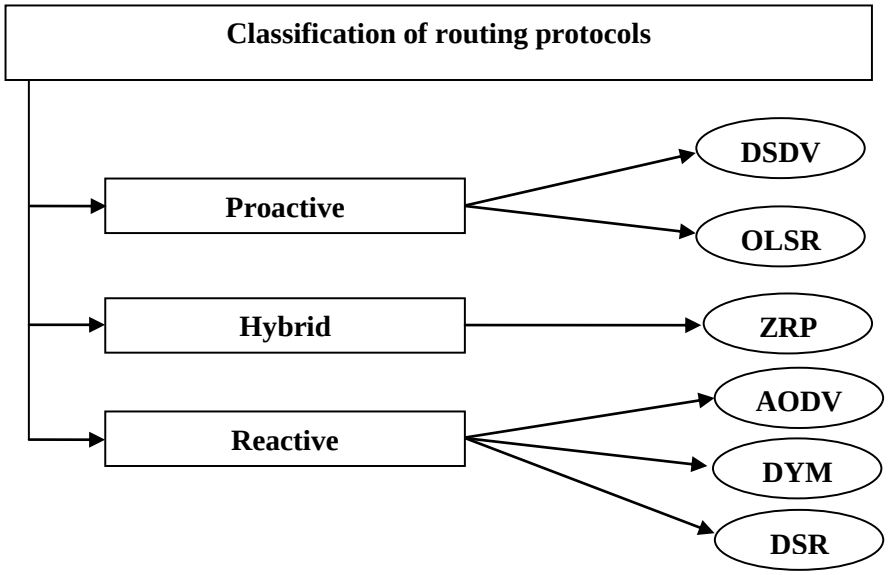

Figure 1. Classification of Routing Protocols

2.1. Proactive Routing Protocols

In proactive routing, each node has one or more tables that contain the latest information of the routes to any node in the network. Each node maintain routing tables and respond to the changes in the network topology by propagating updates throughout the network in order to maintain a consistent view of the network. Many proactive routing protocols have been proposed, for e.g. Destination Sequence Distance Vector (DSDV), Optimized Linked State Routing (OLSR) and so on.

2.2. Reactive Protocols

Unlike proactive routing protocols, the reactive routing protocols create routes once a node wants to transmit data to a destination. The source node initiates route discovery process by flooding route query within the network. When the destination is reached, route reply request will be sent back to the source. Once the route has been found, it is maintained until either destination becomes inaccessible or the route is no longer desired then route discovery process will be invoked again. Several reactive protocols have been proposed such as

Dynamic Source Routing protocol (DSR), Ad hoc On-demand Distance Vector (AODV), and so on.

2.3. Hybrid Routing Protocols

Hybrid routing protocols is combination of proactive and reactive routing protocols, in order to take advantages on these two routing protocols where proactive maintains route in a cluster and reactive maintains route between clusters. Several hybrids routing protocols have been proposed such as Zone Routing Protocol (ZRP), Zone-based Hierarchical Link State (ZHLS) and so on, but the most popular protocol is ZRP.

3. OLSR over View

The Optimized Link State Routing Protocol (OLSR) is developed for mobile ad hoc networks. It operates as a Table driven, proactive protocol, *i.e.,* exchanges topology information with other nodes of the network regularly. Each node selects a set of its neighbor nodes as "multipoint relays" (MPR). In OLSR, only nodes, selected as such MPRs, are responsible for forwarding control traffic, intended for diffusion into the entire network. MPRs provide an efficient mechanism for flooding control traffic by reducing the number of transmissions required.

Figure 2 illustrates a node broadcasting its message throughout the network using regular flooding where all neighbors relay messages and MPR flooding where only MPR nodes relay the messages.

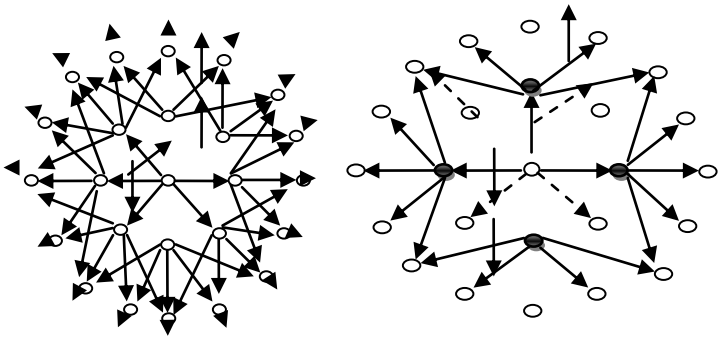

Figure 2. (a) Regular Flooding (b) MPR Flooding

Nodes, selected as MPRs, also have a special responsibility when declaring link state information in the network. Indeed, the only requirement for OLSR to provide shortest path routes to all destinations is that MPR nodes declare link-state information for their MPR selectors. Additional available link-state information may be utilized, *e.g.,* for redundancy. Nodes which have been selected as multipoint relays by some neighbor node(s) announce this information periodically in their control messages. Thereby a node announces to the network, that it has reach ability to the nodes which have selected it as an MPR. In route calculation, the MPRs are used to form the route from a given node to any destination in the network. Furthermore, the protocol uses the MPRs to facilitate efficient flooding of control messages in the network. A node selects MPRs from among its one hop neighbors with "symmetric", *i.e.,* bi directional, linkages. Therefore, selecting the route through MPRs automatically avoids the problems associated with data packet transfer over unidirectional links (such as problem of not getting link-layer acknowledgments for data packets at each hop, for link-layers employing this technique for unicast traffic).

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 is a message that is used for route calculation. In OLSR, each MPR node advertises TC message periodically (every TC INTERVAL). A TC message contains the list of the sender's MPR selector. Figure 3 shows the HELLO and TC Packet format of OLSR

Reserved		Htime	Willingness
Link Code	Reserved	Link Message Size	
Neighbor Interface Address			
Neighbor Interface Address			

Figure 3a. OLSR HELLO Packet Format

Figure 3a Shows HELLO packet format for OLSR. The *Reserved* portion in HELLO packets is used for further modification. *Htime* specifies time before transmission of next HELLO packet. *Willingness* entry specifies node willingness to forward traffic. *Link Code* gives the information about link between sender node and neighbor node. It represents status of neighbor node. *Neighbor interface address* denotes address of interface of neighbor node. *Link Message size* gives total length of link message.

Figure 3b represents TC packet format for OLSR. *Advertised Neighbor Sequence number (ANSN)* which increments sequence number whenever there is change in neighbor set. *Reserved* field is used for further modification in TC packets. *Advertised Neighbor Main Address* field contains main address of neighbor node.

ANSN	Reserved
Advertised Neighbor Main Address	
Advertised Neighbor Main Address	
……..	

Figure 3b. OLSR TC Packet Format

The protocol functioning of OLSR is as follows:

3.1. 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.

3.2. 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.

3.3. 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.

4. 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.

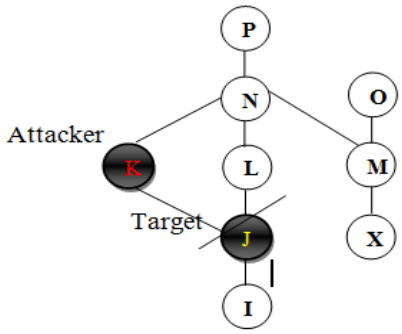

Figure 4. Node Isolation Attack (a) Topology Perceived by Node P before the Attack

In Figure 4(a) Node K is attacking node, and Node J is target node. Instead of sending correct HELLO message {J,N} in neighbors address list the attacker send a fake Hello message that contains{J,N,O,A} which include the target nodes all 2-hop neighbors {N,O} and one non existing node {A}. According to the protocol, the target Node J will select the attacker K as it's only MPR being Node J's the only MPR, the attacker refuse to forward and generate a TC message for Node J. since the link information of the Node J is not propagated to the entire network. Other nodes whose distance to Node J is more than two hopes (*e.g.*, Node P) would not be able to build route to Node J as show in figure 4(b). As a result, other node would not be able to send data to Node J. despite being in the network, and the target Node J will be isolated from the network. An attacker can launch this attack, as long as the target node is within its transmission range.

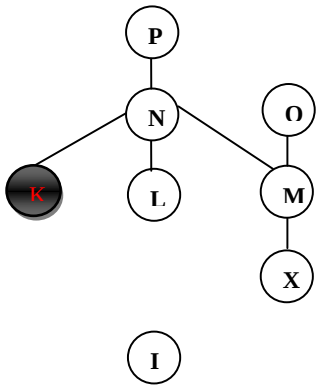

Figure 4(b). Topology Perceived by Node P After the Attack

An attacker can launch this attack, as long as the target node is within its transmission range.

5. **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].

Kurosawa, *et al.*, [15] presented an analysis of black hole attack on AODV protocol. In [15], a passive attack model against AODV protocol has been proposed.

[7, 8, 5] 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.

6. Proposed work

In previous work (EOLSR) node isolated attack is detected but we cannot prevent it from choosing the same attacker node as MPR in future. So we proposed a further improved technique for Enhanced OLSR using the trust based system. Initially all the nodes are assigned high trust value (1.0). Each node maintains the trust value based on the trust value of its neighbors. Then trust value of the nodes is varied according to the activity of the nodes in the network. MPR node is selected based on the trust value of the node. Once the node is detected as attacker using EOLSR, its trust value is reduced to half of its initial value (0.5). Hence in future, selection of attacker as MPR node is prevented since all the nodes will select only high trust node as MPR node. 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. If we found it as malicious then we will assign its trust value as zero. 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 I selects J, K and L as MPR to broadcast packets to M, N, and O and maintains HOP_INFORMATION table show in Table 5.1.

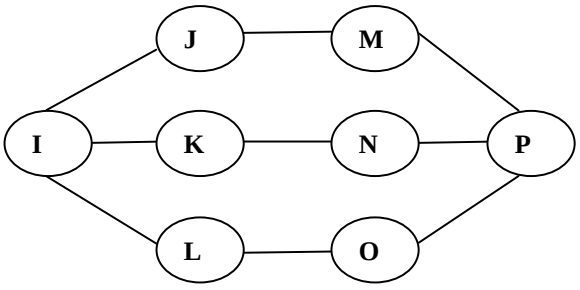

Figure 5.1 OLSR Nodes, I Selects J,K,L as MPR

Table 5.1 I's HOP_INFORMATION

HELLO message sender	2-hop neighbors
J	M
K	N
L	O

In Figure 5.2, if new node Z 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 I add Z's 1-hop information in I's HOP_INFORMATION Table as show in Table 5.3.

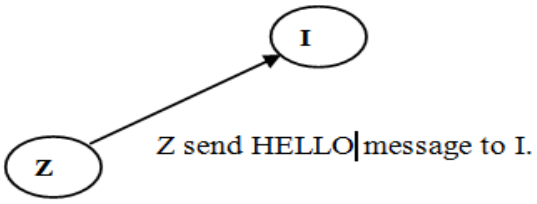

Figure 5.2 Z advertise its Neighbor to I

Table 5.2 Z's HELLO Message

Originator	Neighbors
Z	M,N,O,A

Table 5.3 I's HOP_INFORMATION Table After Receiving Z's HELLO Message

HELLO message sender	2-hop neighbors
J	M
K	N
L	O
Z	M,N,O,A

After including Z's information, (Figure 5.3) A send 2-hop request to its 1-hop neighbors J,K,L and then the node J,K and L forward 2-hop request to their 1-hop neighbor M,N,O to verify whether node Z in its HOP_INFORMATION Table.

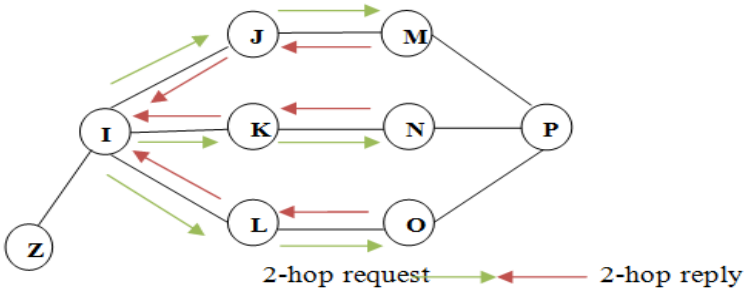

Figure 5.3. I Send 2-hop Request to J, K, L then J, K, L Send Request to M,N,O and M,N,O Send 2-hop Reply to I Through J,K,L.

If node Z founds in the table, then M,N,O sends 2-hop reply to I through J,k,L indicating Z is its 1-hop neighbor. If so, I will select Z as a MPR and broadcast through Z. otherwise I add Z in Blacklist and discard its HELLO message. Node I then informs about the presence of malicious node Z to the network through HELLO and TC messages. And its Trust value is assigned as zero. 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.

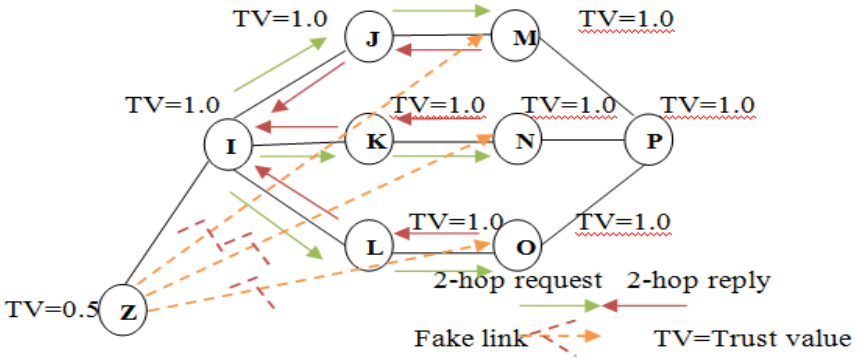

Figure 5.4. Trust Values based on 2-hop Request and Reply

Table 5.4. Trust Value Table

1-hop neighbor of Source	Trust Value
J	1.0
K	1.0
L	1.0
Z	0.5

In other case, if node Z is actually be in the coverage area of M,N,O nodes, then the target node I 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 Z 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 and Algorithm 3 depicts the selection of MPR node.

Due to congestion in the network or node mobility, if any of the two-hop replay is lost, the source 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**

Algorithm 3 : A Trust Value Base Sélection Of MPR.

1. $D_{ij} = [(x_i \sim x_j)^2 + (y_i \sim y_j)^2]^{1/2}$
2. Transmission range = T_x
3. If ($D_{ij} < T_x$) {
4. Node i and Node j are neighbors
5. Neighbors of Node i → N (Node j)
6. }
7. T (i) – Trust value of Node j
8. T (j) – High Trusted neighbor
9. MPR – Multipoint Relay
10. MPR =T (j)

7. Simulation Model and Results

In this section, we present the performance evaluation on our technique using simulation conduct with the network simulator.

SIMULATOR	Network Simulator 2
NUMBER OF NODES	Random
TOPOLOGY	Random
AREA	600 X 600
INTERFACE TYPE	Phy/ Wireless Phy
MAC TYPE	802.11
QUEUE TYPE	Drop tail/ Priority Queue
QUEUE LENGTH	200 Packets
ANTENNA TYPE	Omni Antenna
PROPAGATION TYPE	Two ray Ground
ROUTING PROTOCOL	OLSR
TRANSPORT AGENT	UDP
APPLICATION AGENT	CBR
SIMULATION TIME	50seconds

7.1. Performance Evaluation

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

- *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.
- *Packets loss rate*: It is the number of data packets dropped by the malicious nodes that are selected as MPR nodes.
- *Control packet overhead*: This is the ratio of number of control packet generated to the data packet received.

Figure 6 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 OLSR 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 [17] is 65% which is 5% less than our scheme. This is because the existing solution in [17] 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 [17] is lesser than our scheme.

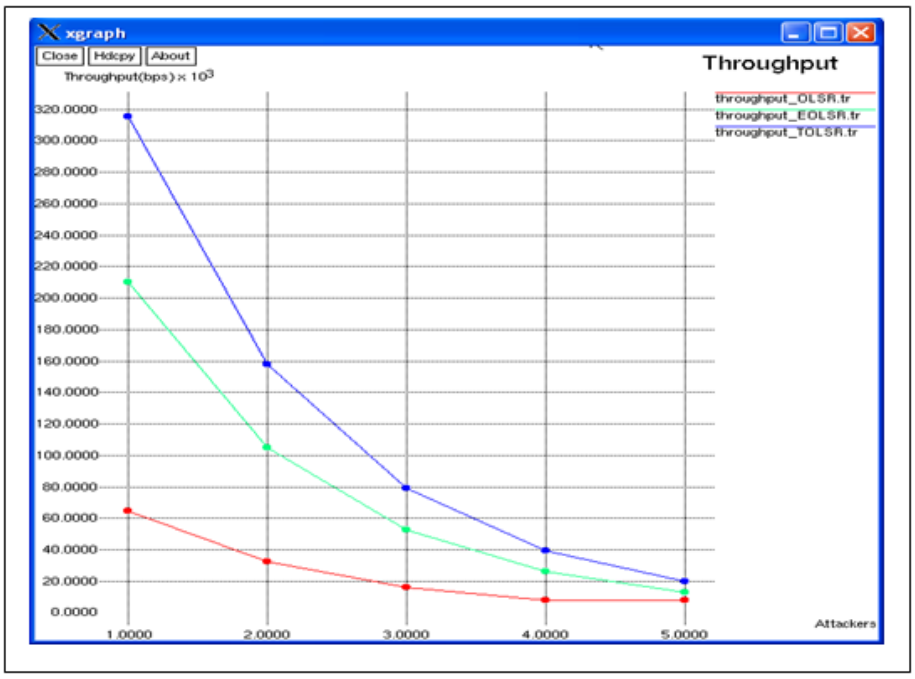

Figure 6. Packet Delivery Ratio

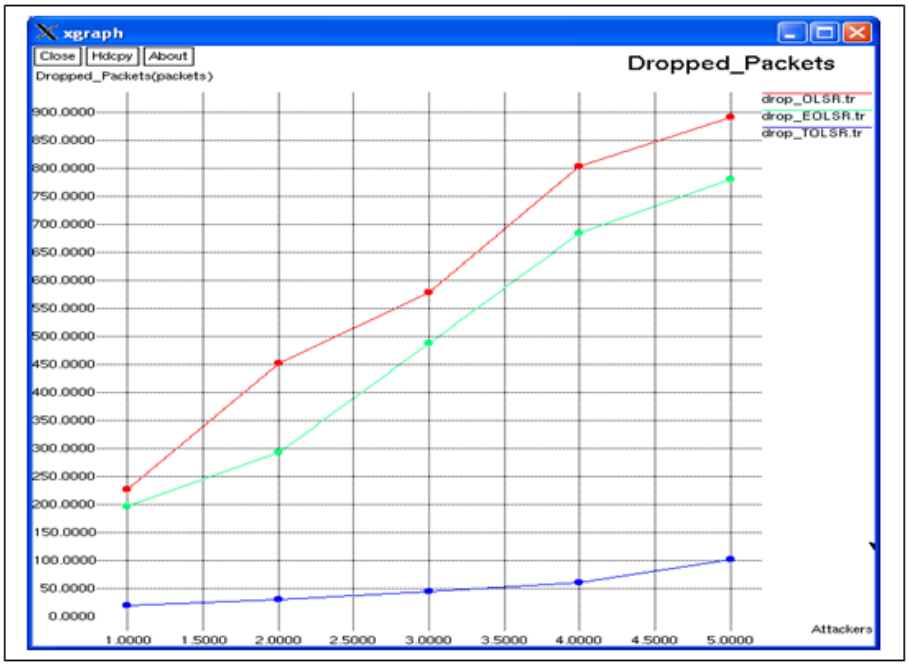

Figure 7. Packet Loss Ratio

Figure 7 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 [17] was approximately 37%, which was increased by 7% when compared to our solution. This is because the existing solution [17] 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 [17]. Moreover, the existing approach in [17] 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 [17].

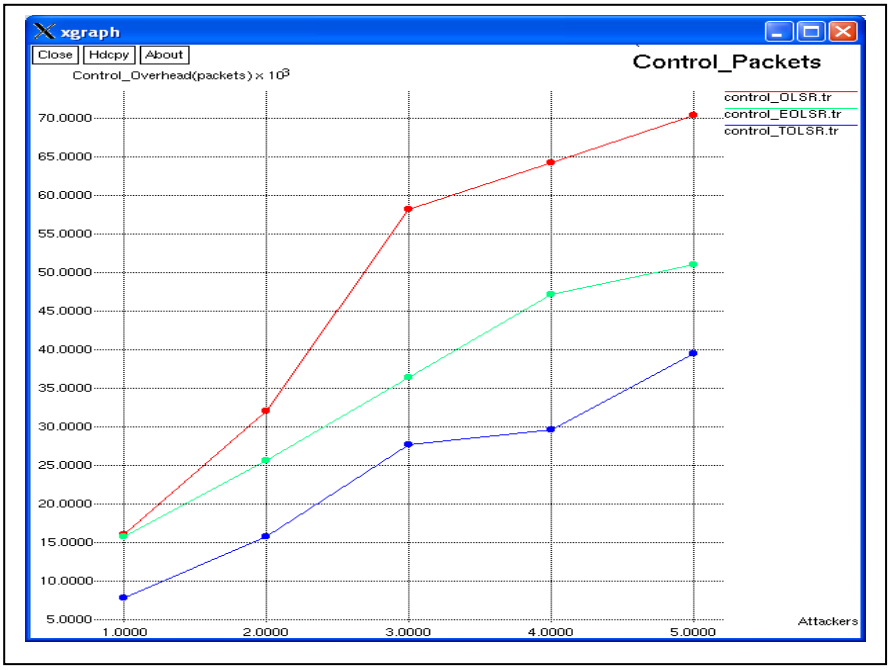

Figure 8. Control Packet Overhead

The control packets ratio of EOLSR is 57% which is 11% higher than the control packet ratio of the solution in [17] which is 46%. This is because of the additional control packets introduced in EOLSR to prevent the node isolation attack by verifying MPR nodes.

8. Conclusion

This work proposes a protocol that provides a defense mechanism against the DOS attack in OLSR MANET protocol. The proposed protocol is named as trust based optimized link state routing (TOLSR), which is based on the existing EOLSR protocol. The proposed TOLSR protocol serves for effective identification of the malicious node that is present in the network. The concept of DOS attack is shown in this work, where a victim node is made not to receive or transmit any messages by the attacker node and thus the delay of response caused by the attacker node on the victim node leads to the isolation of the node that is likely want to become an MPR node. Thus the attacker node succeeds the attempt of DOS attack.

The proposed work aims at preventing the network from this attack by means of verification scheme of hello packets coming from neighbor nodes to detect the malicious nodes and by maintain the trust values for each node in the network. The experiment results show that the percentage of packets received through the proposed work is better than OLSR

in presence of multiple attacker nodes. Throughput of the EOLSR is 62.5 % higher than OLSR and throughput of TOLSR is 46% higher than EOLSR. 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. Packet loss is reduced to less than 100 packets in TOSLR compared to ELOSR and OLSR. Control overhead of TOLSR is 40 % reduced compared to OLSR and EOLSR Moreover, cooperative or colluding attack cannot be launched, because the proposed technique doesn't employ any promiscuous listening of neighbor nodes for detecting the attackers.

References

[1] T. Clausen and P. Jacquet, "RFC3626: Optimized Link State Routing Protocol (OLSR)", Experimental, http://www.ietf.org/rfc/rfc3626.txt.
[2] D. Dhillon and T. Randhawa, "Implementing a Fully distributed Certificate Authority in an OLSR MANET", IEEE WCNC, **(2004)**.
[3] A. Adnane, R. Tim´oteo de Sousa Jr., C. Bidan and L. M´e, "Analysis of the implicit trust within the OLSR Protocol", IFIP International Federation for Information Processing, **(2007)** November.
[4] D. Raffo, C. Adjih, T. Clausen and P. Muhlethaler, "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., **(2004)** October 25.
[5] B. Kannhavong, H. Nakayama and A. Jamalipour, "A survey of Routing Attacks in Mobile Ad hoc Networks", IEEE Wireless Communications, **(2007)** October.
[6] B. Kannhavong, H. Nakayama and A. Jamalipour, "A study of routing attack in OLSR-based mobile ad hoc networks", International Journal of Commnication Systems, **(2007)**, pp. 1241-1261.
[7] F. Hong and L. Hong, "Secure OLSR", Proceedings of the 19th International Conference on Advanced Information networking and Applications, IEEE, **(2005)**.
[8] D. Raffo, "Securing OLSR Using Node Locations," Proc. 2005 Euro. Wireless, Nicosia, Cyprus, **(2005)** April 10–13.
[9] B. Kannhavong, "Analysis of the Node Isolation Attack against OLSR- Based Mobile Ad Hoc Network," 7th International Symposium on Computer Networks, **(2006)**.
[10] P. Ning and K. Sun, "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] Y.-C. Hu, A. Perrig and D. Johnson, "Rushing attacks and defense in wireless ad hoc network routing protocols". ACM Workshop on Wireless Security (WiSe 2003), San Diego, California, U.S.A., **(2003)** September 19.
[12] Y.-C. Hu, A. Perrig and D. Johnson, "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),** pp. 1976–1986.
[13] B. B. W. Wang and Y. Lu, "On vulnerability and protection of ad hoc on-demand distance vector protocol", International Conference on Telecommunication, France, Paris, **(2003)**.
[14] P. Yi, Z. Dai, S. Zhang and Y. Zhong, "A new routing attack in mobile ad hoc networks", International Journal of Information Technology, vol. 11, no. 2, **(2005),** pp. 83–94.
[15] S. Kurosawa, H. Nakayama, N. Kato, Y. Nemoto and A. Jamalipour, "Detecting blackhole attack on AODV-based mobile ad hoc networks by dynamic learning method", International Journal of Network Security, in press, **(2007).**
[16] X. Hong, J. Kong and M. Gerla, "A new set of passive routing attacks in mobile ad hoc networks", Proceedings of IEEE Military Communications Conference (MILCOM'03), Boston, MA, **(2003)** October 13-16.
[17] 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.

