A Trust Based Technique for Defense Against DOS Attack Using Enhanced OLSR in MANET

Dr.T.Manikandan, P.Dharani priya, S.Muthu ranjith kumar,Dr.C.Senthil kumar, N.Nandhini
Assistant Professor, PG scholar, PG scholar Assistant Professor, PG scholar
Department of Computer Science and Engineering
Thiagarajar College of Engineering
Madurai-625015
tmcse@tce.edu, keruba15@gmail.com, ranjith000089@gmail.com, cskcse@tce.edu, nandhunatarajan11@gmail.com

ABSTRACT— **In MANET a proactive algorithm, the Optimized Link State Routing (OLSR) protocol is mostly choose for quite efficient in bandwidth utilization and in path calculation, but it is vulnerable to various attacks. Such as ink withholding attacks & link spoofing attacks, flooding attacks & wormhole attacks , replay attacks & black-hole attacks, colluding misrelay attacks. The node isolation attack is one of the prominent DoS against Optimized Link State Routing Protocol. It occurs when topological knowledge of the network is exploited by an attacker who is able to isolate the victim from the rest of the network and subsequently deny communication services to the victim. As OLSR relies on the cooperation between network nodes, it is easily allow a few colluding or single malicious nodes, and it can cause routing process. In early, Denial contradiction with fictitious node mechanism have been proposed for node isolation attacks, however, these solutions not compromise routing efficiency or network overload due to more nodes are used for fictitious node mechanism, so a new solution named as Enhanced OLSR protocol to defend the Network from node isolation attack for both conditions of with and without contradiction made by 2hop reply and 2hop request and Node existence query, where the protocol has no need additional features of fictitious node mechanism so it can minimize the network lifetime and improve the efficiency of the network system and which proved better performance when compare to all other previous method.**

Keywords: MANET, EOLSR, Node Isolation Attack, NEQ.

I.INTRODUCTION

Mobile Ad Hoc Network (MANET) is a type of network that contains a group of mobile devices which exchanges data. Mobile devices are the nodes in MANET. The nodes in MANET exchange messages through intermediate nodes. Each node in a MANET is free to move independently in any direction at any time. The nodes can join and leave the MANET as they wish. Therefore the communication links between the nodes changes frequently. Each node will act as a router because they deal with the forwarding of data of all other nodes in the network. Each device must continuously maintain the information required to properly route traffic. A number of different routing algorithms exist for network for packet transmission. The algorithms can be classified into two they are proactive and reactive protocols, In the case of proactive are table driven protocol, It maintains a routing table that contains the destinations in the network and the optimal path to the destination. Example for proactive protocols are DSDV [15] and OLSR [11], [12].In Reactive protocols, finds route for message transmission on demand. Example for reactive protocol are DSR [13] and AODV [14], these algorithms differ from the standard routing used in classic networks due to frequent topology changes. A route between two nodes can be broken due to intermediate nodes that dynamically change their position. Mobile nodes can join or leave the network at will, further influencing network connectivity.

In this paper we studied about major DOS attack against the Optimized Link State Routing protocol known as the node isolation attack occurs when topological knowledge of the network is exploited by an attacker who is able to isolate the victim from the rest of the network and consequently deny communication services to the victim. As OLSR relies on the cooperation between network nodes, it is easily allow a few colluding or single malicious nodes, and it can cause routing process. In early, Denial contradiction fictitious node mechanism have been proposed for node isolation attacks, however, these solutions not compromise routing efficiency or network overload due to more nodes are used for fictitious node mechanism, so a new solution named as Enhanced OLSR protocol to defend the Network from node isolation attack for both conditions of with and without contradiction made by 2hop reply and 2hop request and Node existence quire . where the protocol has no need additional features of fictitious node mechanism so it can minimize the network lifetime and improve the efficiency of the network system and which proved better performance when compare to all other previous method.

II. OVERVIEW OF OLSR PROTOCOL

In MANET most widely used protocol is OLSR protocol which is a proactive protocol that maintains a routing table that contains the destinations in the network and the optimal path to the destination. It is efficient in bandwidth utilization and in path calculation. OLSR is the optimization of the classical Link State Routing (LSR) Protocol. It is used to reduce network overhead. Classical Link State Routing Protocol propagates messages by flooding it in the network. This lead to the duplication of messages in the network and thus network overhead is created. In OLSR the duplication and overhead is reduced by selective transmission of data.

The main role in OLSR protocol is selection of MPR (Multi Point Relay).MPRs are the subset of 1-hop neighbors of a node. Through the MPR, a node can access its 2-hop neighbour. OLSR protocol achieves optimization by appointing minimum number of MPRs for a node. Nodes selected as MPRs are those which has connection with maximum number of 2-hop neighbors. MPRs are the forwarding agents for control packets throughout the network. A node will select an MPR only if it covers all the 2-hop neighbors of the node. The minimal MPR set is the forwarding agent that allows forwarding of control messages and data packets by less duplication and also covering the whole network. There are two types of messages used they are hello and topology control (TC) messages to discover and then disseminate link state information throughout the mobile ad hoc network. all nodes in the network makes use of shortest hop forwarding paths and Individual nodes use this topology information to compute next hop destinations, Here HELLO message will declare a node's knowledge about its surroundings. It list out the 1-hop neighbors of the node. A node broadcast their HELLO message in the network. Other nodes that receive and respond to the HELLO message are the 1-hop neighbors of the sender node. Neighbor nodes know each other by exchanging HELLO messages, which reflect the local connectivity. HELLO messages are used in the selection of the MPR set for routing connectivity. TC message lists out the nodes that had made the sender as their MPR. Nodes maintain the topology based on HELLO and TC messages.

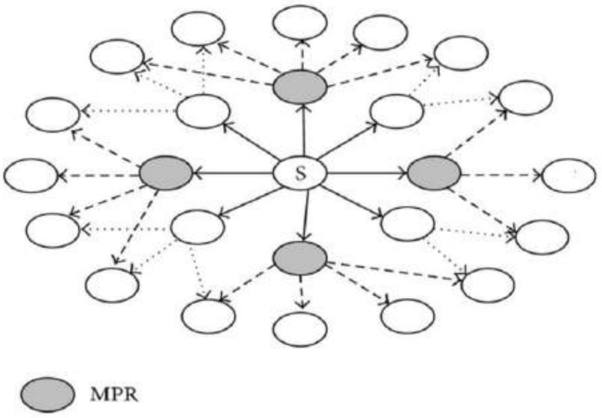


Figure 1: MPR selection in OLSR protocol

A. HELLO Message and Topology control Message

In OLSR protocol which uses HELLO message and TC(Topology control) message, Each node generates HELLO message periodically that contains its own address and the list its 1-hop neighbours.

A TC(Topology control) message that used for Route calculation, and it is advertised by MPR periodically. A TC message contains the list of the sender's MPR selector.

B. Neighbour Sensing

In neighbour sensing, the HELLO message are broadcasted periodically. The HELLO messages are broadcast only to one hop neighbour. These messages are used to obtain the information about neighbours. A HELLO message performs the task of neighbour sensing and MPR selection process. A node's HELLO message contains its own address, a list of its 1-hop neighbours 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 neighbours and can find out which node has chosen it as an MPR.

C.MPR Flooding

The main role of OLSR protocol is MPR Flooding, It is a process of transmitting data from source node to destination node through entire network. Each node designates, from among its bi-directional neighbours, a MPR set such that a message transmitted by the node and relayed by the MPR set is received by all its 2-hop neighbours.

Nodes send their HELO messages as to intimate "willingness" for the selection of MPR, which is taken into consideration for the MPR calculation. Each node selects its MPR set from among its 1-hop neighbours such that they can reach all its 2-hop neighbours. Each node maintains information about the set of neighbours that have selected it as an MPR. The set of nodes having selected a given node as MPR is the MPR-selector-set of that node. A node obtains this information from periodic HELLO messages received from the neighbors. In OLSR, each MPR node must forward the data and routing message coming from any of its MPR selectors.

III.NODE ISOLATION ATTACK

OLSR protocol is vulnerable to many types of attacks. Node isolation attack is such an attack that is capable to compromise OLSR protocol. It is a type of Denial of Service (DoS) attack. DoS attack is an attempt to make a network resource unavailable to its intended users, such as to temporarily or indefinitely interrupt or suspend services of a host connected to the Internet. In node isolation attack an attacker purposely isolates a victim node from the network. In this attack, the attacker exploits the fact that a node always prefers the minimal set of MPRs. In order to attack the victim the attacker will send a fake HELLO message to the attacker. This HELLO message claims that the sender node is in close proximity to all of the victim's 2-hop neighbours. It also advertises a fictitious node in order to attain the belief of victim. Therefore, according to the MPR selection rules the victim will appoint the attacker as its MPR. Then the attacker will not include the victim in its TC message. And this fraudulent MPR will not forward any messages from the victim to other nodes in the network. Thus the victim will get isolated in the network.

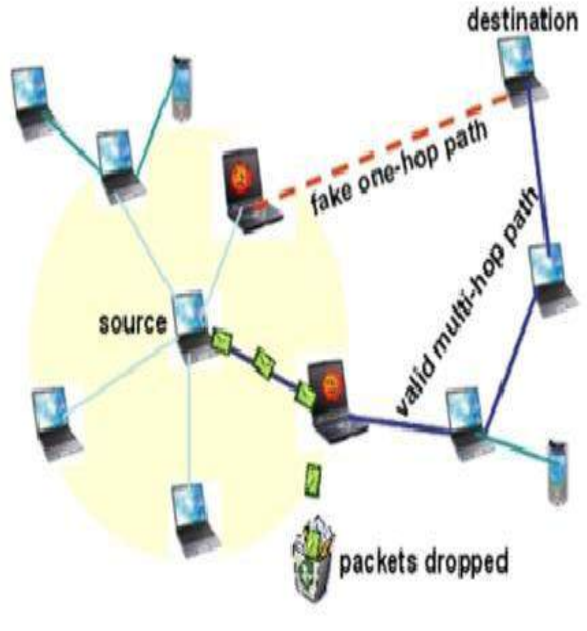


Figure 2: Node Isolation Attack

IV. PROPOSEDWORK

In existing work to avoid node ISOLATION ATTACK using Fictitious node Mechanism these solutions not compromise routing efficiency or network overload due to more nodes are used for fictitious node mechanism.

The proposed solution named as Enhanced OLSR routing protocol to defend the Network from node isolation attack, which will be able to detect the presence of malicious nodes in the network. Even though our proposed solution is based on our previous work, we have modified the approach of detecting the malicious node. This is to eliminate any malicious node from giving the false information about any normal node that wants to become MPR. Our solution assumes that all the nodes are authenticated and can participate in communication that is all nodes are authorized nodes for both conditions of with and without contradiction made by 2-hop reply and 2-hop request and Node existence query. where the protocol has no need additional features of fictitious node mechanism so it can minimize the network lifetime and improve the efficiency of the network system and which proved better performance when compare to all other previous method.

Proposed method uses

- 2-HOP REQUEST
- 2-HOP REPLY
- NODE EXISTENCE QUERY

In OLSR nodes trust all information that received from its 1-hop neighbour. Here we analyze the pattern of Hello message of the node that advertise all 2-hop neighbours as its 1-hop neighbours and verify whether that node is malicious or not, here TC and HELLO message are used to select MPR and route calculation. Each node in the network periodically broadcasts their HELLO message to indicate its presence. In this mechanism, each node maintains HOP_INFORMATION table which contains of HELLO message sender and its 2-hop neighbours.

In the proposed methodology, steps are involved they are

Step 1: L selects A,B and C as MPR to broadcast packets to T,U,V and maintains HOP_INFORMATION table

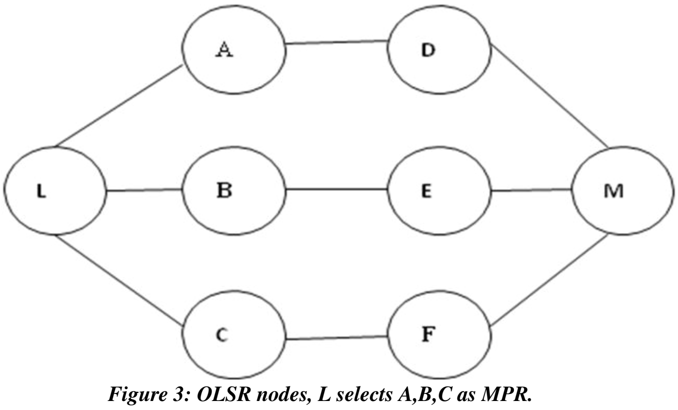


Figure 3: OLSR nodes, L selects A,B,C as MPR.

TABLE 1: L's HOP_INFORMATION

HELLO message sender	2-HOP neighbour
A	D
B	E
C	F

Step 2:when new node Y comes, it sends HELLO message as advertising all the targe node L's 2-hop neighbors as its 1-hop neighbors along with new neighbor Z to source node.

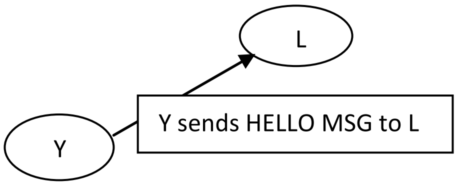


Figure 4: Y advertise its neighbour to L

Step 3: Then L add Y's 1-hop information in L's HOP_INFORMATION table.

Table 2: Y's HELLO message

Originator	neighbours
Y	D,E,F,Z

Table 3:L's HOP_INFORMATION table after receiving Y's HELLO message

HELLO message sender	2-HOP neighbours
A	D
B	E
C	F
Y	D,E,F,Z

Step 4:After including Y's information, Z send 2-hop request to its 1-hop neighbors A,B,C and then node A,B,C forward 2-hop request to their 1-hop neighbor D,E,F to verify node Y in its HOP_INFORMATION table.

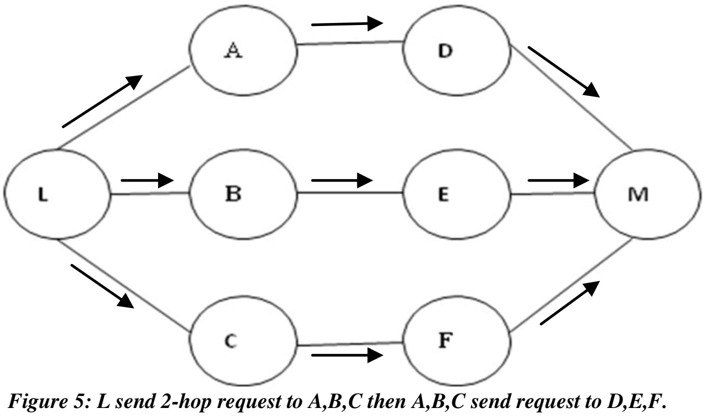


Figure 5: L send 2-hop request to A,B,C then A,B,C send request to D,E,F.

Step 5:If node Y in the table,then D,E,T sends 2-hop reply to L through A,B,C indicating Y is its 1-hop neighbor.

Step 6:Then source node select Y as MPR, otherwise L add Y in Blacklist and discard it.

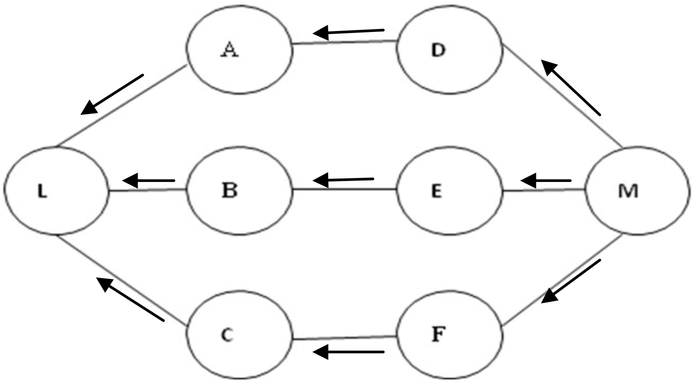


Figure 6: D,E,F send 2-hop reply to L through A,B,C.

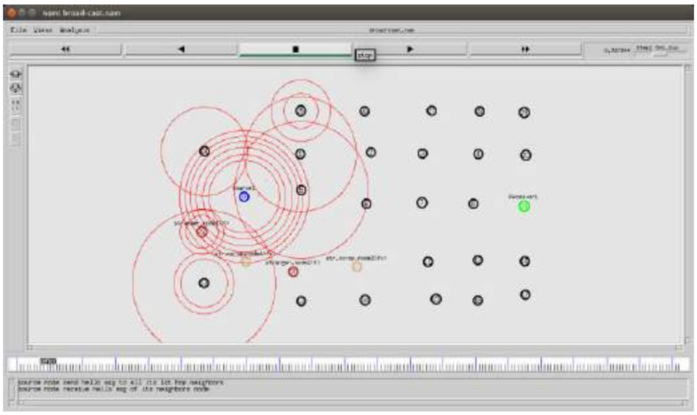
Step 7:If node Y is actually be in the coverage area of T,U,V nodes, Targeted node L sends NEQ(Node Existence Query) message to entire network through current MPR.

Step 8:If any designated MPR node confirms the existence of node A,then it will be selected as MPR,otherwise node Y will be Detected and Discarded.

V .SIMULATION AND RESULTS

5.1 Simulation

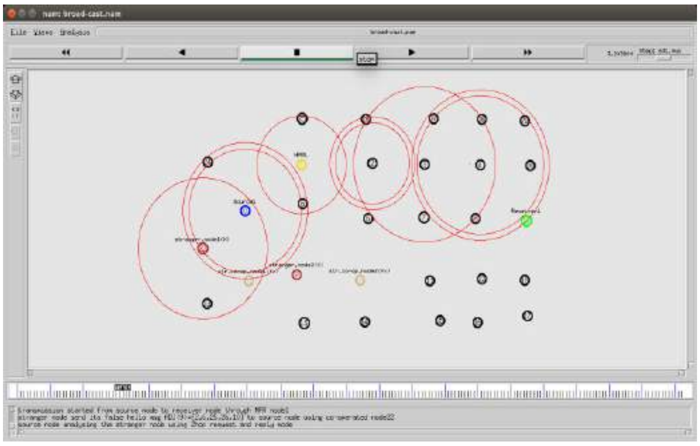
In this section, the performance evaluation on our technique was simulated using Network simulator NS2.3 Here in simulation 30 Nodes are created, here the victim node sends hello message to its 1st hop neighbour, after receiving hello message from victim node, the 1st hop neighbour node will send reply message to victim node.



```
source node send hello msg to all its 1st hop neighbors
source node receive hello msg of its neighbors node
```

Figure 7:Source Node send and receive HELLO message to its neighbour

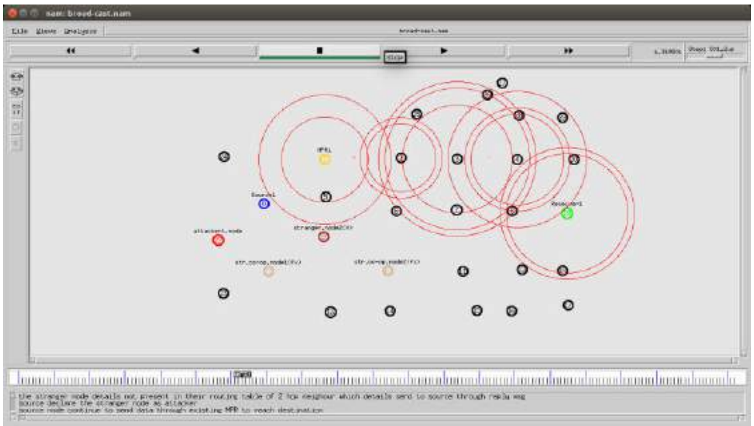
Based on OLSR protocol MRP will be selected, which are designated as forwarding agents for control packets throughout the network. MPRs are selected as a subset of its 1-hop neighbours, such that the MPR set allows coverage of all of its 2-hop neighbours. By minimizing its MPR selections, a node is able to transmit messages to all 2-hop neighbours with minimal duplicate. Thus, both topology control messages and data packets are only forwarded by this minimal MPR set, allowing for less duplicate messages while maintaining network-wide coverage.



```
transmission started from source node to receiver node through MPR node1
stranger node send its false hello msg HELLO(9)->(2,6,25,26,10) to source node using co-operated node22
source node analysing the stranger node using 2hop request and reply mode
```

Figure 8:Transmission Starts through MPR

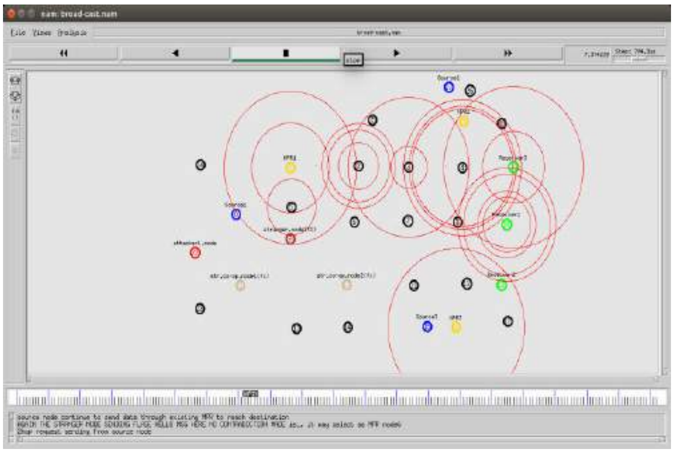
There are two types of messages used to find out network topology in OLSR HELLO and TC. The HELLO message, which declares a node's knowledge of its adjacent, is broadcast to all. Any node can broadcast and reciprocate back to the sender is classified as a 1-hop neighbour, then each node acquires its local topology up to a 2-hop range. OLSR requires that all nodes selected as MPRs periodically advertise a TC message register all nodes that have selected the sender as its MPR. The control messages are only propagated through the MPR, reducing overall network traffic.



```
the stranger node details not present in their routing table of 2 hop neighbour which details send to source through reply msg
source declare the stranger node as attacker
source node continue to send data through existing MPR to reach destination
```

Figure 9:Stranger node sends fake HELLO message

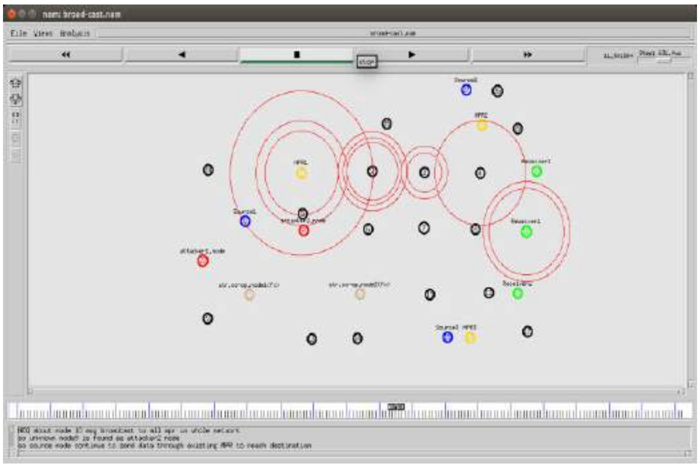
The stranger node sends False hello message to select as MPR and get the data from victim node. This fake message will be predicted by victim using EOLSR technique that is victim node analysis the stranger node using 2-HOP request and 2-HOP reply node,if stranger node details not present in their routing table of 2-HOP neighbour,that details sends to victim node through reply message then victim node declare the stranger node as attacker node and selects another MPR to send data from source node to destination node.



```
source node continue to send data through existing MPR to reach destination
AGAIN THE STRANGER NODE SENDING FLASE HELLO MSG HERE NO CONTRADICTION MADE so... it may select as MPR node6
2hop request sending from source node
```

Figure 10:Source node declare stranger node as attacker node and again stranger node sends Fake HELLO message in without Contradiction

In without contradiction technique again the stranger node sends fake HELLO message,at this time victim node send NEQ(node existence query) to all the current MPR to entire network, if it is not present then victim node isolate the Attacker node from the network.



```
NEQ about node 15 msg broadcast to all mpr in whole network
so unknown node5 is found as attacker2 node
so source node continue to send data through existing MPR to reach destination
```

Figure 11: Stranger node found as attacker through NEQ and 2-hop request and reply

5.2 RESULT AND DISCUSSION

A. Packet Delivery Ratio

The ratio between the number of packets sent by the CBR sources of source nodes and the number of packets received by the CBR sink at the destination node.

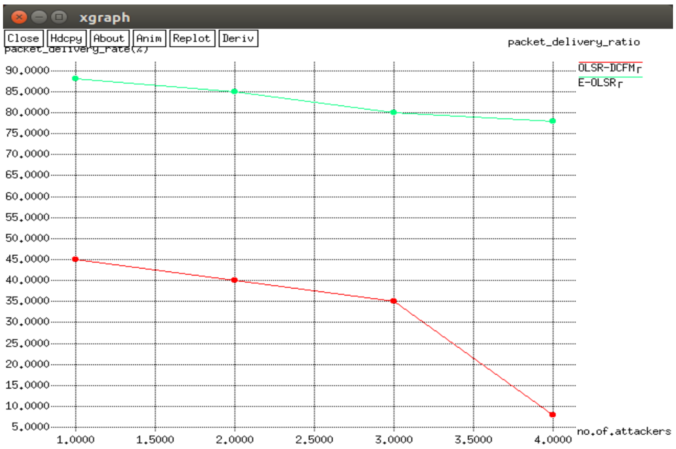


Figure 12:Packet Delivery Ratio

Figure 12: 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. Each of these nodes analyzes the TC messages and hello messages from their neighbouring nodes , selects them as a victim, they create a fake hello message containing all the 2-hop neighbours 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, so we are calculating the packet delivery ratio

X-axis represents the packet delivery ratio and Y-axis represents no of attackers, here we are comparing existing with proposed protocol, when comparing with existing OLSR protocol no of packet delivery ratio is increased in proposed Enhanced OLSR protocol.

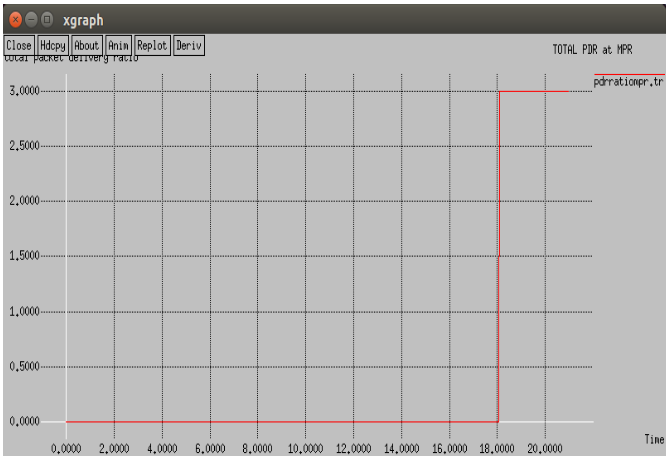


Figure 13:Total Packet Delivery Ratio

X-axis represents the packet delivery ratio and Y-axis represents time, here we are comparing total packet delivery ratio at MPR nodes. This graph is generated through trace file values.

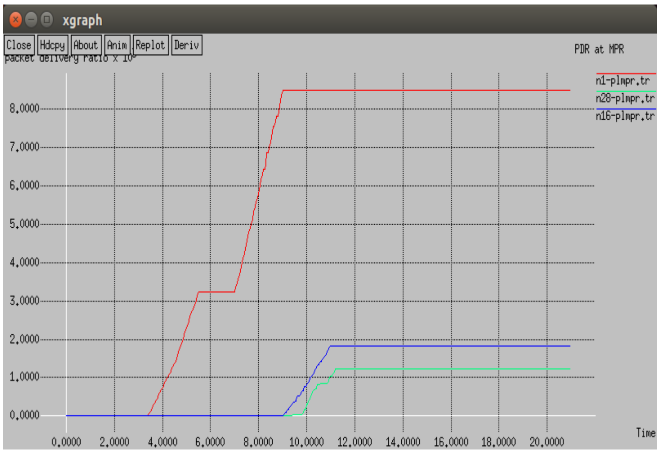


Figure 14: Packet delivery ratio at MPR nodes

X-axis represents the packet delivery ratio and Y-axis represents time, here we are comparing three nodes they are node 1,node 28 and node 16.

B. Packet Loss Rate

It is the number of data packets dropped by the malicious nodes that are selected as MPR nodes.

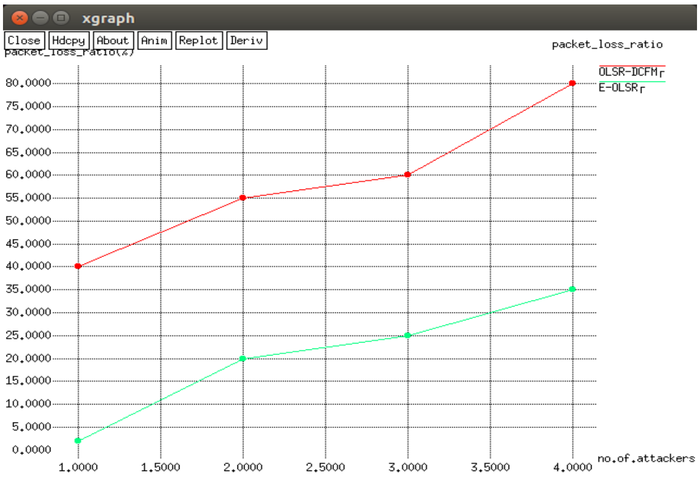


Figure 15:Packet Loss Ratio

Figure 15: shows the number of packets dropped by the malicious nodes in OLSR and EOLSR. The packet loss rate of OLSR under attack was approximately 74%, while the packet loss rate of EOLSR was approximately 30%.

X-axis represents the packet loss ratio and Y-axis represents no of attackers, here we are comparing existing with proposed protocol, when comparing with existing OLSR protocol no of packet loss ratio is decreased in proposed Enhanced OLSR protocol.

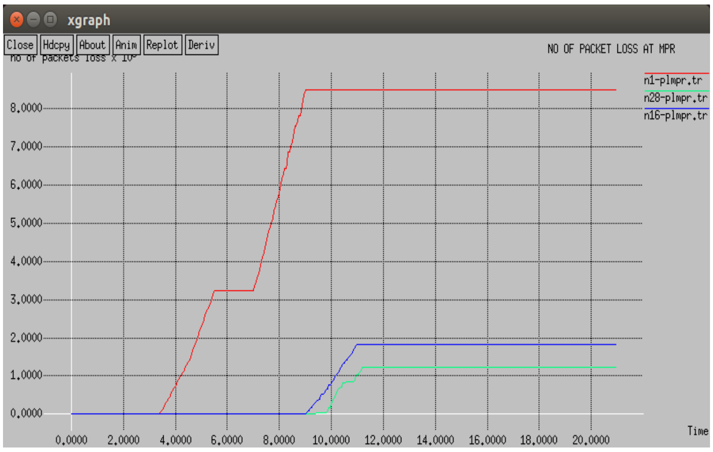


Figure 16:No of Packet Loss At MPR nodes

X-axis represents the packet Loss ratio and Y-axis represents time, here we are comparing three nodes they are node1,node 28 and node 16.This graph is generated through trace file values.

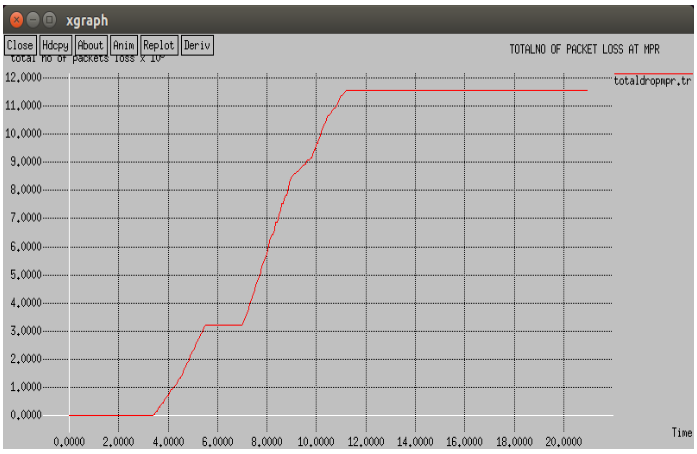


Figure 17: Total No of Packet Loss

X-axis represents the total packet Loss ratio and Y-axis represents time, here we are comparing total packet loss ratio at MPR nodes only. This values are generated through trace file values.

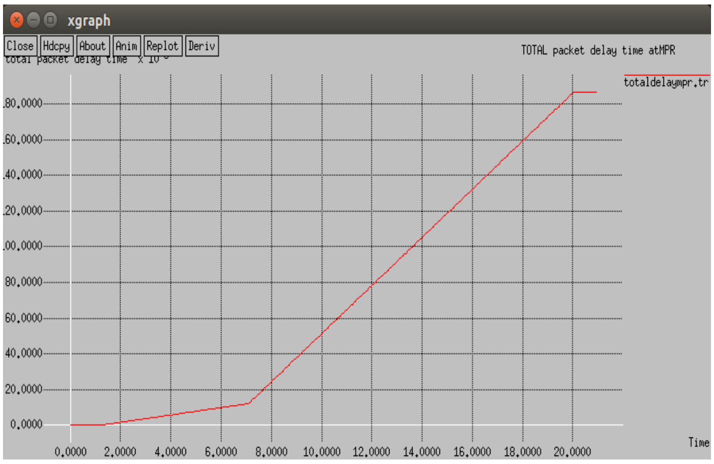


Figure 18: Total Packet Delay Time at MPR

X-axis represents the packet Delay time ratio and Y-axis represents time, here we are comparing total packet delay time at MPR Nodes.

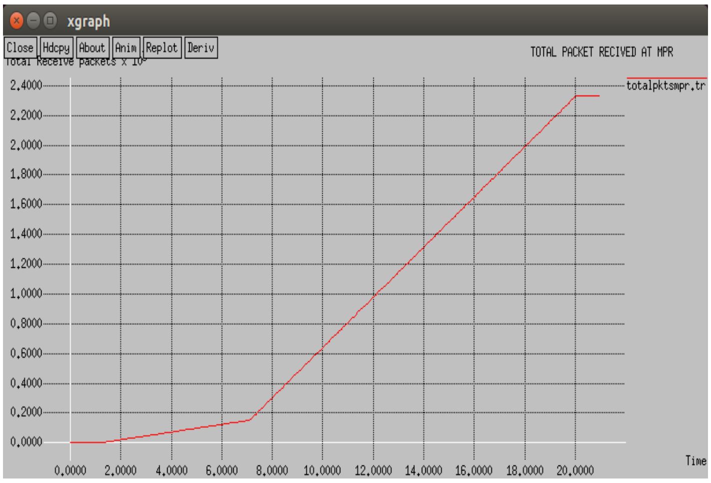


Figure 19: Total Packet Received at MPR

X-axis represents the total packet Received ratio and Y-axis represents time, here we are comparing total packet Received time at MPR Nodes.

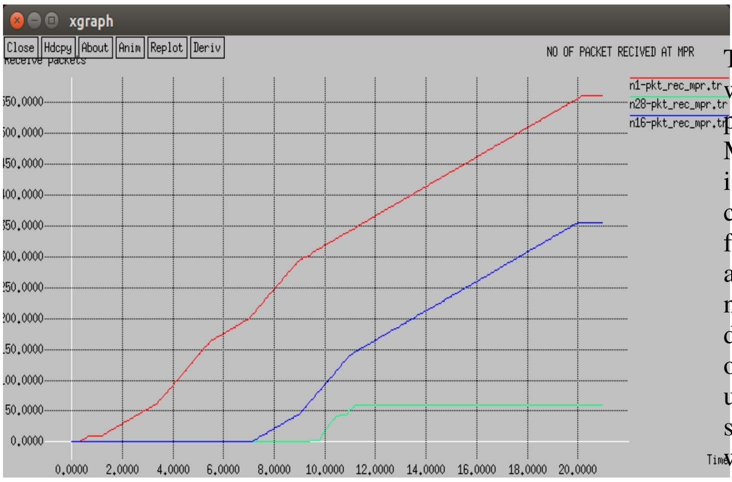


Figure 20: No of packet received at MPR nodes

X-axis represents the packet received ratio and Y-axis represents no of nodes, here we are comparing three nodes they are node1,node 28 and node 16.

C. Control Packet Overhead

This is the ratio of number of control packets generated to the data packet received.

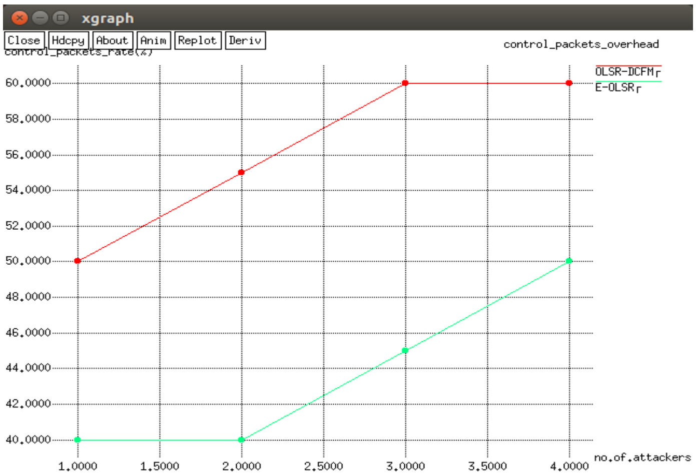


Figure 21:Control Packet Overhead

X-axis represents the control packet rate and Y-axis represents no of attackers, here we are comparing existing with proposed protocol, when comparing with existing OLSR protocol control packet overhead is decreased in proposed Enhanced OLSR protocol.

VI.CONCLUSION

This project focuses on preventing node isolation attack, which is nothing but Denial of Service (DoS) attack in OLSR protocol. Denial Contradictions with Fictitious Node Mechanism (DCFM) is the method used to prevent node isolation attack. The DCFM method suggests three contradiction rules to avoid the attack. DCFM also use a fictitious node in order to identify attacker who was somehow able to follow the contradiction rules. Thus DCFM prevent node isolation attack in OLSR protocols but this mechanism depends more node so it leads to poor network lifetime but its overcome by a new improved enhanced techniques where used 2hop reply and 2hop request and NEQ, where Simulation shows that enhanced olsr successfully prevents the attack, in which all nodes. Finally we compare the output of proposed system using ns2 simulator and it shown the better output result when compare to existing method.

REFERENCES

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

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

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

[4] A. Nadeem and M. Howarth, “A survey of manet intrusion detection & prevention approaches for network layer attacks,” Communications Surveys Tutorials, IEEE, vol. 15, no. 4, pp. 2027–2045, Fourth 2013.

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

[6] A. Adnane, C. Bidan, and R. de Sousa, "Trust-based countermeasures for securing olsr protocol," in Computational Science and Engineering,2009. CSE '09. International Conference on, vol. 2, Aug 2009, pp. 745-752.

[7] E. Gerhards-Padilla, N. Aschenbruck, P. Martini, M. Jahnke, and J. Tolle, "Detecting black hole attacks in tactical manets using topology graphs," in Local Computer Networks,2007. LCN 2007. 32nd IEEE Conference on, Oct 2007, pp. 1043-1052.

[8] B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato, and A. Jamalipour, "A survey of routing attacks in mobile ad hoc networks," Wireless Communications, IEEE, vol. 14, no.13
5, pp. 85-91, October 2007.

[9] D. Dhillon, J. Zhu, J. Richards, and T. Randhawa, "Implementation evaluation of an ids to safeguard olsr integrity in manets,"in Proceedings of the 2006 International Conference on Wireless Communications and Mobile Computing, ser. IWCMC 06. New York, NY, USA:ACM, 2006, pp. 45-50.

[10] Y.-C. Hu, A. Perrig, and D. Johnson, "Wormhole attacks in wireless networks," Selected Areas in Communications, IEEE Journal on, vol. 24, no. 2, pp. 370-380, Feb 2006.

[11] H.L.Nguyen,U.T.Nguyen, “Study of Different Types of Attacks on Multicast in Mobile Ad Hoc Networks,” International Conference on Networking, Systems, Mobile Communications and Learning Technologies, Apr,2006.

[12] C. Adjih, D. Raffo, and P. Muhlethaler, "Attacks against olsr: Distributed key management for security," in 2nd OLSR Interop/Workshop,Palaiseau, France, 2005.

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

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

[15] 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.

[16] H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang, “Security in mobile ad hoc networks: challenges and solutions,” Wireless Communications, IEEE, vol. 11, no. 1, pp. 38–47, Feb 2004.

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

[18] P. Jacquet, P. Muhlethaler, T. Clausen, A. Laouiti, A. Qayyum, and L. Viennot, “Optimized link state routing protocol for ad hoc networks,” in Multi Topic Conference, 2001. IEEE INMIC 2001. Technology for the 21st Century. Proceedings. IEEE International, 2001, pp. 62–68.

[19] T. Clausen and P. Jacquet, “RFC 3626 - Optimized Link State Routing Protocol (OLSR),” p. 75, 2003. [Online]. Available: http: //www.ietf.org/rfc/rfc3626.txt

[20] D. Johnson, Y. Hu, and D. Maltz, “Rfc: 4728,” The dynamic source routing protocol (DSR) for mobile ad hoc networks for IPV4, 2007.

[21] C. Perkins and E. Royer, “Ad-hoc on-demand distance vector routing,” in Mobile Computing Systems and Applications, 1999. Proceedings WMCSA ’99. Second IEEE Workshop on, Feb 1999, pp. 90–100.

[22] C. E. Perkins and P. Bhagwat, “Highly dynamic destination sequenced distance-vector routing (dsdv) for mobile computers,” in Proceedings of the Conference on Communications Architectures, Protocols and Applications, ser. SIGCOMM ’94. New York, NY, USA: ACM, 1994, pp. 234-244.[Online]:http://doi.acm.org/10.1145/190314.190336.

[23] M. Omar, Y. Challal, and A. Bouabdallah, “Reliable and fully distributed trust model for mobile ad hoc networks,” Computers & Security, vol. 28, pp. 199 – 214, 2009. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S016740480800117X