ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2015

A Secure OLSR against Dos Attack in Ad-Hoc Networks

Megha Eileen Varghese[1], Perumal Sankar[2]

PG Student [Wireless Technology], Dept. of ECE, Toc H Institute of Science and Technology, Kochi, India[1]

Professor, Dept. of ECE, Toc H Institute of Science and Technology, Kochi, India[2]

ABSTRACT: A mobile adhoc network (MANET) is a group of self-configuring, infrastructureless network of mobile devices that are connected by wireless links. In MANETs, nodes not only acts as host, but also acts as routers to forward messages between the nodes that are within the direct communication range and also to other nodes that are not within the direct transmission range with the help of intermediate nodes. MANETs have constantly changing topology and also lack incorporation of security features in statistically configured wireless networks because of which, they are prone to suffer from malicious behaviours than traditional wired networks.Since MANET assumes a trusted environment for routing, security is a major issue. In this paper, we consider a specific type of DoS attack called as the node isolation attack in OLSR, a proactive routing protocol. A technique called Eliminating Malicious node in OLSR (EM-OLSR) is considered in which we detect and eliminate the malicious node in the network with the help of control packets and then protect these packets using Hardy algorithm.

KEYWORDS: MANET, Optimized Link State Routing (OLSR), Node Isolation attack.

I.INTRODUCTION

A mobile ad hoc network (MANET) is a collection of mobile devices that can communicate with each other without the use of a predefined infrastructure or centralized administration. In MANETs there are nodes which acts both as host and router to forward messages to other nodes that are in different wireless transmission range. MANETs can be constructed quickly at low cost as it does not rely on existing infrastructure; they have a constantly changing topology. Thus, MANETs have their application in disaster relief, emergency operations, military service, maritime communications, vehicle networks, campus networks, robot networks. Compared to the conventional network, MANETs have dynamic, continually changing topology which makes it difficult to perform routing. The main drawbacks of MANET are that, they have limited bandwidth, limited battery power and also susceptible to various kinds of security threats.

Routing protocols in MANET can be classified into two categories: proactive protocol, reactive protocol and hybrid protocol that makes use of properties of both proactive and reactive protocol. Proactive protocols are based on periodic exchange of control messages. The proactive protocols immediately provide the required routes when needed, at the cost of bandwidth used in sending frequent periodic updates of topology. The examples of this kind of protocols are DSDV and OLSR. In reactive routing protocol, it does not take the initiative for finding a route to a destination, until it is required. The protocol attempts to discover routes only “on-demand” by flooding its query in the network. This type of protocols reduces control traffic overhead at the cost of increased latency in finding the route to a destination. The examples of this kind of protocols are AODV, DSR and TORA. Optimized link state routing (OLSR) protocol, a proactive routing protocol offers promising performance in terms of bandwidth and traffic overhead which does not incorporate any security measures. Thus OLSR is vulnerable to various kinds of attacks such as flooding attack, link withholding attack, replay attack, denial-of-service (DOS) attack and colluding misrelay attack. Among these, DOS attack is one of the major attack in which some nodes do not co-operate with ad-hoc networks thereby resulting in denial of service (DOS) and such nodes are termed as malicious nodes.

There are many previous and existing works done in order to alleviate these attacks. Some of the countermeasures used are: (i) cryptographic approach (ii) key management methods (iii) signature and timestamp schemes and (iv)cooperative security. In the proposed paper, a mechanism called Eliminating Malicious node in OLSR (EM-OLSR)

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2015

protocol, which is a trust based technique is used to secure the OLSR nodes against the denial of service (DoS) attack. In a hostile environment, a malicious node can launch routing attacks to disrupt routing operations or denial-of-service (DoS) attacks to deny services to legitimate nodes.

II.BACKGROUND AND PROBLEM ANALYSIS

I. BACKGROUND

Optimized Link State Routing: The Optimized Link State Routing (OLSR) protocol is table driven, proactive routing protocol designed for mobile ad hoc networks. It employs periodic exchange of messages to maintain topology information of the network at each node. Based on topology information, each node is able to calculate the optimal route to a destination. In OLSR, routes are immediately available when needed. The key concept of the protocol is the use of "multipoint relays" (MPR). Each node selects a set of its neighbour nodes as MPR. Only nodes, selected as such MPRs, are responsible for generating and forwarding topology information, intended for diffusion into the entire network. MPRs provide an efficient mechanism for flooding topology information by reducing the number of transmissions required [1]

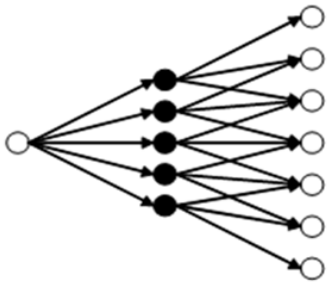

Fig.1The broadcast from the leftmost node is retransmitted by all its neighbours [3]

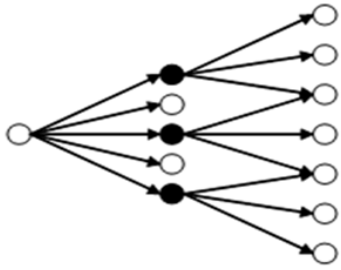

Fig. 2 The broadcast from the leftmost node is retransmitted by its MPRs only [3]

Nodes which have been selected as multipoint relays by some neighbour node(s) announce this information periodically in their control messages. Thereby a node announces to the network, that it has reachability 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 neighbours with "symmetric", i.e., bi-directional, linkages. Therefore, selecting the route through MPRs automatically avoids the problems associated with data packet transfer over uni-directional links (such as the problem of not getting link-layer acknowledgments for data packets at each hop, for link-layers employing this technique for unicast traffic).The core functionality of OLSR includes neighbour sensing, multipoint relays selection and topology diffusion.[1]

III. PROBLEM ANALYSIS

Node Isolation Attack: DoS attacks are active attacks in which malicious nodes generate false messages in order to disrupt the network's operations or to consume other nodes' resources. Node isolation attack is a kind of DOS attack launched by malicious nodes against OLSR protocol. The goal of this attack is to isolate a node from communicating

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2015

with other nodes in the network. More specifically, this attack prevents a victim node from receiving data packets from other nodes in the network. The idea of this attack is that attacker(s) prevent link information of a specific node or a group of nodes from being spread to the whole network. Thus, other nodes who could not receive link information of these target nodes will not be able to build a route to these target nodes and hence will not be able to send data to these nodes [2].

In this attack, attacker creates virtual links by sending fake HELLO messages including the address list of target node's 2-hop neighbours, (the attacker can learn victim's 2-hop neighbours, by analysing TC message of its 1-hop neighbours). According to OLSR protocol, the MPR selection is based on the maximum coverage of any node's 2-hop neighbours. So the target node will select the attacker to be its only MPR node because it assumes that it can reach all its 2-hop neighbours through the attacker itself. Thus, the only node that must forward and generate TC messages for the target node is the attacking node. By dropping TC messages received from the target and not generating TC messages for the target node, the attacker can prevent the link information of target node from being disseminated to the whole network. As a result, other nodes would not be able to receive link information of a target node and will conclude that a target node does not exist in the network thus launching DOS attack on the victim [2].

Therefore, a target node's address will be removed from other nodes' routing tables. Since in OLSR, through HELLO messages each node can obtain only information about its 1-hop and 2-hop neighbours, other nodes that are more than two hops away from a 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 [2].

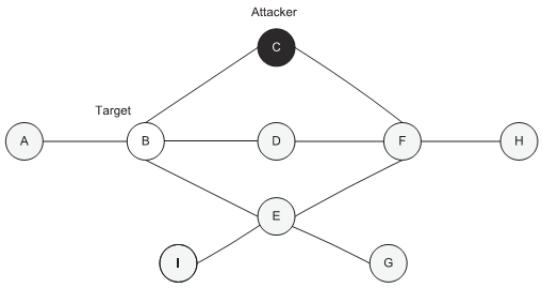

Fig. 3 Topology perceived by node H before the attack [2]

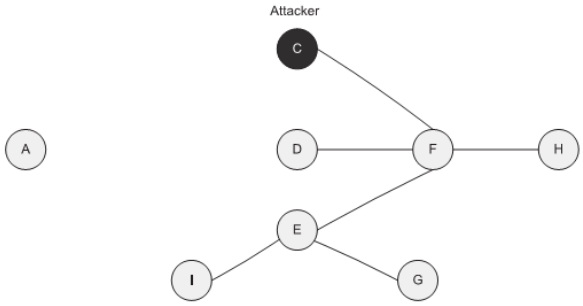

Fig. 4 Topology perceived by node H after the attack [2]

In Fig.3, node C is the attacking node, and node B is the target node. Instead of sending correct HELLO message that contain {B, F} in neighbour address list, the attacker sends a fake HELLO message that contains {B, F, G, Z} which includes the target node's all 2-hop neighbours {F, G}and one non-existent node {Z}. According to the protocol, the target node B will select the attacker C as it's only MPR. Here node Z is announced only by the attacker and not by any other neighbour nodes of the victim. This is to improve the possibility of attacker being selected as a MPR. So the victim node B assumes that its 2-hop neighbour node Z can be reached only via node C (attacker) and all the other 2-

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2015

hop neighbours also can be reached through node C itself. So it selects node C as it's only MPR. Being node B's only MPR, the attacker refuses to forward and generate TC message for node B. Since the link information of node B is not propagated to the entire network, other nodes whose distance to node B is more than two hops (e.g., node H) would not be able to build route to node B.

Fig.4 shows the topology perceive by node H after the node isolation attack . As a result, other nodes would not be able to send data to node B. Despite being in the network, the target node B will be isolated from the network. An attacker can launch this attack, as long as the target node is within its transmission range.

IV. RELATED WORKS

In [4] they found that DoS attacks are much easier to launch on wireless networks than on wired networks. This is typically due to the nature of wireless communication as packets frantically move around in the air. This paper also comprehensively explained different DoS attack and also explained a set of effective defense mechanisms, further, the paper also proposed some mechanism against ARP poisoning and IDS or IPS architecture that could help against such attacks.

In [5] they modelled, simulated and verified a variant of the Optimized Link State Routing (OLSR) protocol, named Reliable (R-OLSR) to detect and isolate selfish behaviour during packet forwarding. The main contribution is the traffic monitoring in time on each multiple relay point (MRP).

[3] introduced a new routing attack, called Node Isolation attack, against OLSR-based mobile ad hoc network was presented. This attack allows attacker(s) to isolate a specific node or a group of nodes from receiving data packets from other nodes who is further than two hops. They proposed a simple technique to detect the attack as the first step to defend against the attack. One shortcoming of the proposed solution was that it employs promiscuous listening to overhear packets forwarded by the MPR nodes which results in energy dropping at the individual nodes and that it might not detect the attack in which two consecutive nodes work in collusion [7].

[6] explains SEAD protocol which is established based on one way hash function chain faster than asymmetric key cryptography and avoiding some attack such as Denial of Service (DoS) attack and uncoordinated attack. They also explain about the Aridane (Secure On-Demand Routing Protocol for Ad-hoc Networks) which assurances that the destination node authenticates to the source node and the source node authenticate to each intermediate node in each path. Every intermediate node can delete or add nodes in the list of nodes of the route request.

[7] explains about the countermeasures against the DoS attack. Firstly it explains about the anti-DoS service called AID, which has a random peer to peer network that connects the registered client network with registered servers even when they are under DoS attack. Secondly they explain about the perimeter based defence against DDoS attack where they identify the sources of attack and install appropriate rate-limit filters on the edge routers connecting to the flooding sources.

V. PROPOSED MODEL

In [2] we can see a static topology taken into consideration while in our proposed model called EM-OLSR we take a dynamic topology. In this paper we detect the presence of the malicious node, remove this malicious node simultaneously removing these nodes from the routing table. Then we protect the packets using Hardy function, inorder to prevent any future attack. In [2] alongwith the Hello messages and the Topology Control (TC) messages three other control packets called 2-hop request, 2-hop reply, Node Exist Query(NEQ) are also considered. Consider a specific node "A" in a network. The node would already know its one hop and two hop neighbours. Now, consider an unknown node "X" who wants to get into the network. This unknown node X, in its routing table will show that its one hope neighbours are same as the two hop neighbours of the node A who wants to transmit the data packets. Now node A will select node X as the Multipoint Relay(MPR). Inorder to check the authenticity of such a node, 2-hop request is send by node A. The 2-hop neighbours of A then would send a 2-hop reply. If node X is present in all the 2-hop reply it receives, A will select X as a MPR and broadcast all the data and TC packets through node X to the other part of the network. Otherwise node X would be deleted from the routing table informing the other nodes in the network about the

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2015

presence of the malicious node. If the node X actually exists, then the node A queries about the existence of the one hop neighbour of node X through the current MPR nodes. If those one hop neighbours are found in the list of MPR nodes, then the presence of node X is confirmed. After this process, the final route to the destination would be secured by Hardy function, a simple encryption-decryption method. HARDY is hierarchical password based key derivation function [8] in this users (password pass as a constant string s, Ic1,L=128 bit(symmetric key) and master key pass as MP(plain text message), encryption function E[], number of round n, all are pass as a input). Here the various characters are converted to the ascii value.

The proposed model is done in 3 steps.

Step 1: Hello reception[2]

Step 2: 2-Hop request reception[2]

Step 3: Hardy function[8]

VI. SIMULATION AND RESULTS

The simulation was done in network simulator 2 [9]. A random topology with 60 nodes were taken. The dimension of 5770×100m was considered. Maximum transmission range of each node was 250m. The duration of the simulation was 15s. The malicious nodes were chosen randomly. The traffic type was CBR.

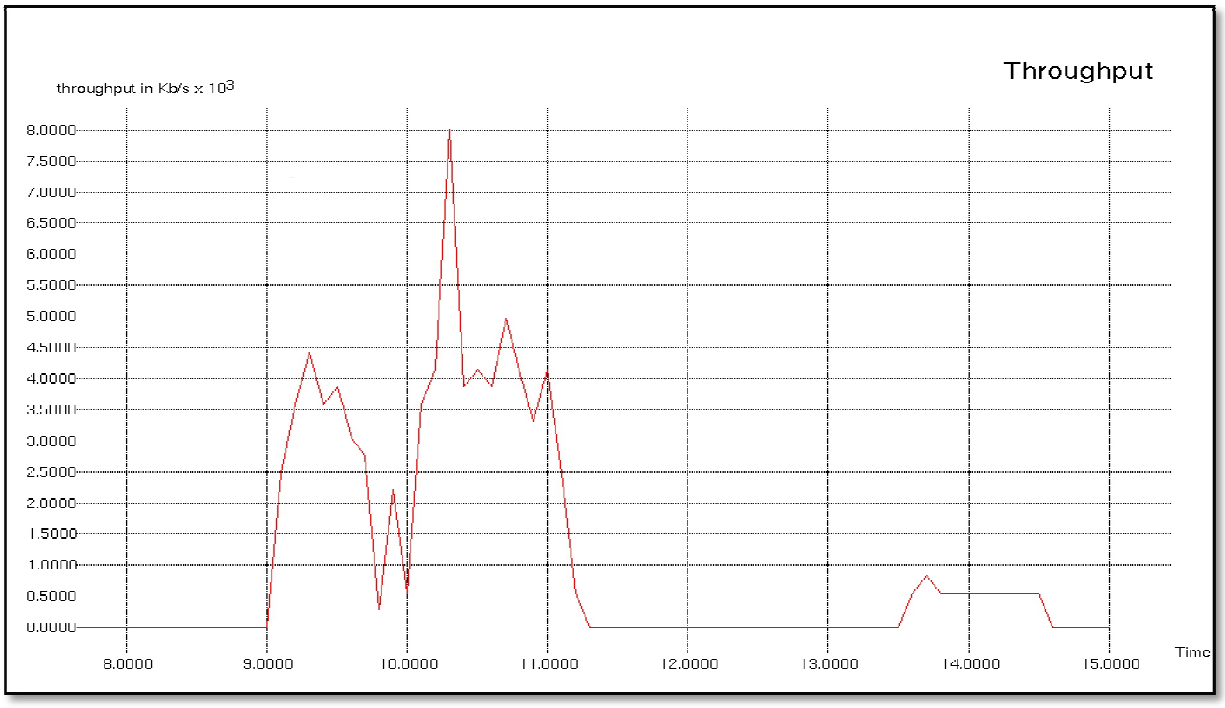

Fig. 5 Throughput of destination node

Here the throughput graph of the destination node is shown. X-axis represents the timewhile Y-axis represents throughput. From the 9th sec to the 11th sec the data transmission takes place. After the 11th sec the malicious nodes are detected in the network and these nodes are removed. So, at that time the destination node would not get the data packets which makes the throughput zero. From 13.5th sec retransmission of the data happens through the secure new route.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2015

VII. CONCLUSION

Mobile Ad Hoc Networks (MANETs) form a class of dynamic multi-hop networks consisting of a set of mobile nodes that intercommunicate on shared wireless channels. A MANET node can move freely within network communication range, and server as a router and host which can forward data packets to other hosts according to configured routing protocol. MANETs are self-organizing and self-configuring multihop wireless networks, where the network structure changes dynamically due to the node mobility. There exists no fixed topology due to the mobility of nodes, interference. MANETs are much more vulnerable and are susceptible to various kinds of security attacks because of its cooperating environment.

Optimized link state routing (OLSR) routing, a proactive routing protocol, which offers a better performance in terms of bandwidth and traffic overhead but it fails to incorporate any security measures. As a result, OLSR is vulnerable to various kinds of attacks such as flooding attack, link withholding attack, replay attack, denial-of-service (DOS) attack and colluding misrelay attack. The vulnerabilities of a pro-active routing protocol called optimized link state routing (OLSR) against a specific type of denial-of-service (DOS) attack called node isolation attack is considered. The nodes that do not co-operate or disrupt the network are termed as malicious node. A mechanism called Eliminating Malicious node in OLSR (EM-OLSR) protocol which is expected to be a trust based technique is used to secure the OLSR nodes against the attack, followed by protecting the packets using Hardy function, a simple encryption-decryption method. For this proposed project, the various simulations were done in NS2.

REFERENCES

[1] T. Clausen and P. Jacquet, "IETF RFC3626: Optimized link state routing protocol (OLSR),"Experimental, 2003.
[2] MohanapriyaMarimuthuandIlangoKrishnamurth" Enhanced OLSR for Defense against DOS Attack in Ad Hoc Networks" Journal Of Communications And Networks, Vol. 15, No. 1, pp. 31-37,February 2013.
[3] B. Kannhavong, H. Nakayama, N. Kato, Y. Nemoto, and A. Jamalipour,"Analysis of the node isolation attack against OLSR-based mobile ad hoc network," inProc. ISCN, pp. 30–35,2006.
[4] Lawan A. Mohammed and BijuIssacDoS " Attacks and Defense Mechanisms in Wireless Networks" Mobile Technology, Applications and Systems, 2005 2nd International Conference on 15-17, 8 pp. – 8, Nov. 2005
[5] A.Lekova, Mo Adda "Reliable OLSR In Manets For Detecting And Isolating User Selfish Nodes" Complex Control Systems, Institute of Systems Engineering and Robotics ISSN 1310 – 8255, 2012.
[6] MojtabaGhanaatPishehSanaei, Imran Ghani, Aida Hakemi, SeungRyulJeong, "Routing Attacks In Mobile Ad Hoc Networks: An Overview" Sci.Int.(Lahore),25(4),pp.1031-1034,2013.
[7] S.Meenakshi, "Comprehensive Mitigation Mechanism AgainstDDos Attack –A Comprehensive Study", Asian journal of information technology 5(7): pp.691-695, 2006.
[8] KhaleelMershad and Hassan Artail, "A Framework for Secure and Efficient Data Acquisition in Vehicular Ad Hoc Networks" IEEE Transactions On Vehicular Technology, VOL. 62, NO. 2, pp. 536-551, February2013
[9] The network simulator version 2 (NS2). Home page http://www.isi.edu/nsnam/NS2/