Fictitious Node Deployment to Prevent Routing Attacks on OLSR Protocol

M.Sitharam J[1], Mohan Sasidhar[2]
[1]*Research Scholar, Department of CS &SE,College of Engineering(A),AndhraUniversity,Visakhapatnam,India*
[2]*P.G. Scholar, Department of CS & SE, College of Engineering (A), Andhra University,Visakhapatnam, India*

Abstract-With the main focus of research in routing protocols for Mobile Ad-Hoc Networks (MANET) geared towards routing efficiency, the resulting protocols tend to be vulnerable to various attacks. Different solutions have been proposed for different types of attacks, however, these solutions often compromise routing efficiency or network overload. One major DOS attack against the Optimized Link State Routing protocol (OLSR) known as the node isolation attack occurs when topological knowledge of the network is exploited by an attacker. The use of infrastructure free network such as MANET has increased tremendously. In such environment, the security is more important because the data should keep safe and the identification of Node isolation and wormhole attackers should begin earlier, the performance of the network should be increased by mitigating those attacks at the earlier stage. The above stated points are the main objective of this Paper. It finds the attack made by the Hackers.

Keywords- Mobile Ad-hoc Networks, OLSR protocol, DOS attack, Security

I. INTRODUCTION

Ad-Hoc networks have free infrastructure where the nodes are free to join and left the network at any time. The nodes are connected with each other via a wireless link in Ad-Hoc network. In this free infrastructure, a node can act as a server as well as client to transmit the data in the network. Therefore this kind of network is also known as infrastructure less networks. These networks have no centralized server or authority. Routing and channel selection are also on demand. Whenever a node in the network is inactive or moves from the network, that causes the link failure. The source node will establish a new channel. Ad-Hoc network can be categorized in to two types named as Mobile Ad-Hoc network (MANET) and Vehicular Ad-hoc networks. Every mobile node can communicate with each other directly if a contact occurs. Every node performs the same and supports this cooperation, due to the intention of reducing communication cost. Due to this flexible nature, there are several security issue threatens ad-hoc networks. Ad-Hoc networks have the capabilities to handle those issues in different ways.

Different types of routing algorithms exist for network packet transmission with security constraints. In general, the routing algorithms in MANET can be classified into three main categories, such as reactive routing and proactive routing protocols and hybrid routing protocols. Inthe case of proactive which is also known as table- driven protocol, for example, DSDV and OLSReach node persistently maintains a list of all possible destinations in the network and the optimal paths routing to it. Reactive protocols, named as DSR (Dynamic Source Routing) and AODV (Ad-hoc On Demand Distance Vector). The on-demand routing protocols are not predefined the route and these protocols will find a route between source and destination only when the demand arises. The final one is hybrid protocol, Researchers believe that the issue of efficient operation over a wide range of conditions can be addressed by a hybrid routing method, where the proactive and the reactive behavior is combined in the amounts that best match these `operational environments. Representative hybrid routing protocols includes Zone Routing Protocol (ZRP) and Zone-based Hierarchical Link State routing protocol (ZHLS), these are the popular hybrid protocols available in MANET.

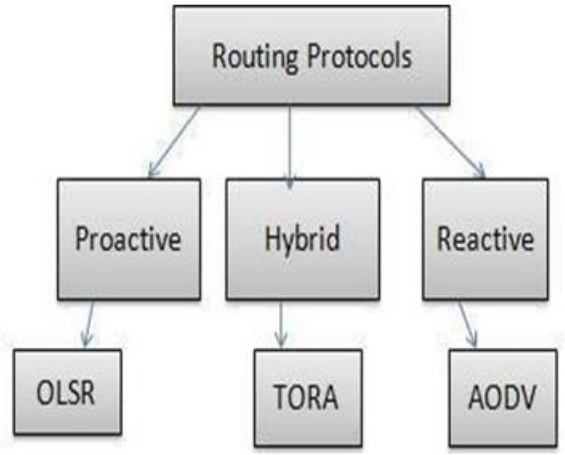

Fig.1: Flow chart of Routing Protocols

i. OLSRProtocol:

The Optimized Link State Routing protocol (OLSR) is a proactive link state routing protocol. In OLSR routing protocol, there are two types of control packets used
Hello packets and Topology Control packets (TC).

Hello packets are used to build theneighborhood of a node and to discover the nodes that are within the environs of the node. And this also used to compute the multi-hop relays of a node. The OLSR protocol uses the periodic broadcast of hello packets to establish the connection.

The Hello messages are received by all one- hop neighbors, but the Hello messages are not forwarded to other nodes by the received node. This hello message broadcasting will happen for every fixed interval; this is known as Hello interval. This allows the nodes to discover its two-hop neighbors since the node can passively listen to the

transmission of its one-hop neighbor. The status of these links with the other nodes in its neighborhood can be asymmetric, symmetric or Multi Point Relay (MPR).The main advantage of using OLSR is it does not require that the link reliable for the control messages. The messages will be sentperiodically and the delivery does not have to be sequential. This is more suitable for the application, which needs fastdata transmission of the data packets with low delay.

The main process of OLSR is as follows.

- Neighborsensing
- MPR (Multi PointRelay)selection
- MPR information declaration
- Route tablecalculation.

II. RELATED WORK

In [11] J. Yi, A. Adnane, S. David, and B. Parrein proposed Multipath routing protocols for Mobile Ad hoc NETwork (MANET) address the problem of scalability, security (confidentiality and integrity), lifetime of networks, instability of wireless transmissions, and their adaptation to applications. The protocol, called MultiPath OLSR (MP-OLSR), is a multi-path routing protocol based on OLSR. The *Multipath Dijkstra Algorithm* is proposed to obtain multiple paths. The algorithm gains great flexibility and extensibility by employing different link metrics and cost functions. In addition, *route recovery* and *loop detection* are implemented in MP-OLSR in order to improve quality of service regarding OLSR. The backward compatibility with OLSR based on IP source routing is also studied. Simulation based on Qualnet simulator is performed in different scenarios. A testbed is also set up to validate the protocol in real world.

In [12] Kannhavong et al. attempt to mitigate the problem of colluding attackers. By modifying the HELLO message to include all 2-hop neighbors, a node can detect existing contradictions between messages, thus identifying an attack. Of course, as the authors themselves noted, it is difficult to distinguish between contradictions which occur due to an attack as opposed to those resulting from topology changes. In addition, such contradictions identify an attack but fail to identify theculprit.

Raffo et al. [13] proposed a mechanism to improve the security of the OLSR routing protocol against external attackers. In their solution, each node signs its HELLO and TC messages. These signatures are later used by others to prove their own HELLO and TC messages. The resulting solution prevents devices from declaring imaginary links with known nodes. This solution functions correctly but is expensive in terms of overhead; besides the usual overhead of OLSR, signing messages requires extensive computation, a cumulative factor that grows as the size of the networkincreases.

III. IMPLEMENTATION

a. EXISTING SYSTEM:

Kannhavong et al. attempt to mitigate the problem of colluding attackers. By modifying the HELLO message to include all two-hop neighbors, a node can detect existing contradictions between messages, thus identifying an attack.

Raffo et al. propose a mechanism to improve the security of the OLSR routing protocol against external attackers. In their solution, each node signs its HELLO and TC messages.

DISADVANTAGES:

It is difficult to distinguish between contradictions which occur due to an attack as opposed to those resulting from topology changes.

b. PROPOSEDSYSTEM:

A Specific DOS attack called Node Isolation Attack and a new mitigation method is proposed. Our solution called Denial Contradictions with Fictitious Node Mechanism (DCFM) relies on the internal knowledge acquired by each node during routine routing, and augmentation of virtual (fictitious) nodes. Moreover, DCFM utilizes the same techniques used by the attack in order to prevent it. The overhead of the additional virtual nodes diminishes as networksize increases, which is consistent with general claim that OLSR functions best on large networks. We further strengthened the attack by giving the attacker the ability to follow the victimaround.

c. METHODOLOGY:

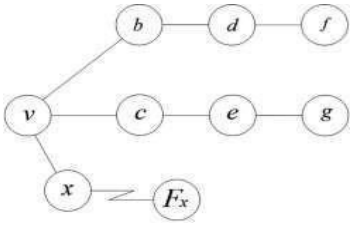

Fig.2: Identifying contradictions to prevent node isolationattack

In this section we describe the rules that must be satisfied in order for a node to deem a HELLO message's sender trustworthy.

Consider fig 2 where ADJ(v) = {b, c ,x}and ADJ2(v) = {d, e}.

Based on OLSR , v must select MPR'(v)= {b, c} so that ADJ2(v) is covered.

Suppose x is interested in isolating victim v.

According to the attack presented, x declares a fake HELLO message containing ADJ(x)= $\{v, d, e, F\}_x$.

x wouldn't declare {b, c} ADJ(v), because v could verify this by comparing x's HELLO with the HELLO messages of b andc.

Therefore, the first rule is:

When node x advertises a HELLO message containing ADJ(x), v should confirm that all of thenodes declared by x are not among ADJ(v).

This can be accomplished by checking earlier HELLO messages to see whether or not they report the sender as their

neighbor.

- As nodes b and c must exist in ADJ2(x), x must select MPRs that will allow it to reach these nodes. It might be the case, however, that x will pretend that it wants to choose v itself as MPR for covering b and c. Based on OLSR's, v cannot refuse. Under such a scenario, v cannot conclude that x is being malicious. However, v can check whether x appointed some other MPR for covering nodes in ADJ2(x) {b, c}, namely either d or e.

This brings us to the second rule:

- For each node y mentioned in a HELLO message, v should examine whether there exists z ADJ(y),s

that (a) it is not mentioned in the sender's HELLO message and (b) is located at least three hops away from v. If these conditions are fulfilled, another examination is needed: (c) has x appointed w ADJ(x) as MPR for covering z?

Using Fictitious Nodes

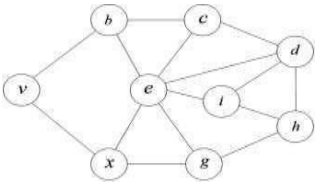

Fig.3: An Example of node isolation attack with no Contradictions

Consider Fig.2 in which x advertises that ADJ(x) = {v,e,c,g} lying about the node c. ADJ2(x) = {b, c, d, i, h}, and v cannot identify any contradictionbecause:

- x doesn't claim to know any node, other than itself, contained in ADJ(v) (rule No.1),
- x appointed MPRs for reaching all of ADJ2(x), namely, {b, c, d, i,h}.

Thus, it is expected that x wouldn't appoint c as one of its MPRs, as d is already reachable by e, and x doesn't claim to know all of ADJ(v), specifically {b}.

Let us define a fictitious node, Fz

- As a node declared by node z that doesn't actuallyexist.
- Fz is not declared fictitious, causing all other nodes believe it's a realnode.
- This implies that all nodes will have an entry for Fz in their routing table and all routes from or to Fz must pass through z.

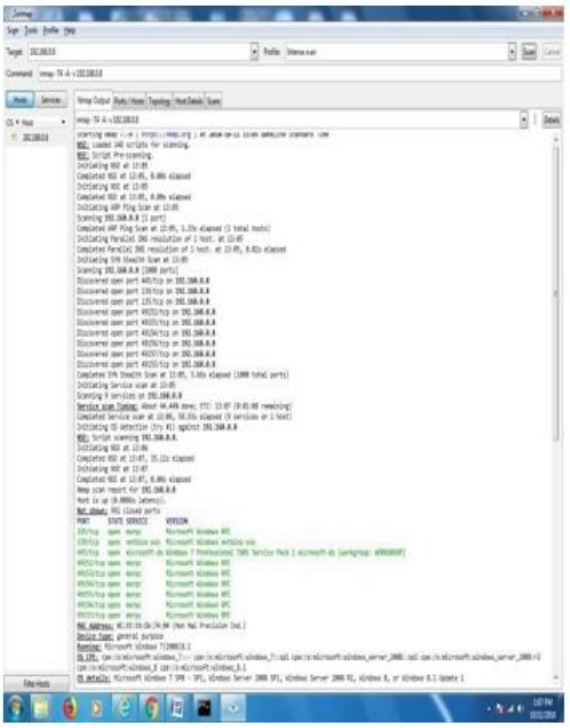

Fig.4: Scanning the openports

IV. RESULTS

Fig.5: Pcap file of theattacker

Fig.6: Evaluating the pcap files using the python code

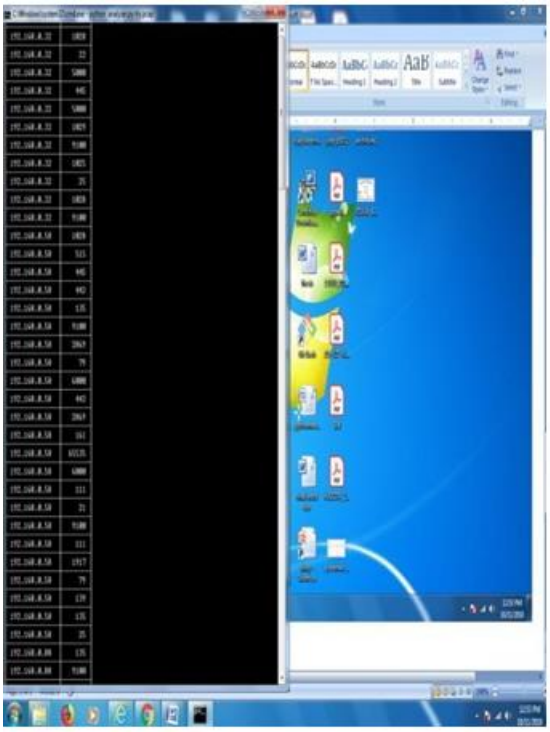

Fig.7: Evaluating no. of times user tried access the port using the fictious node

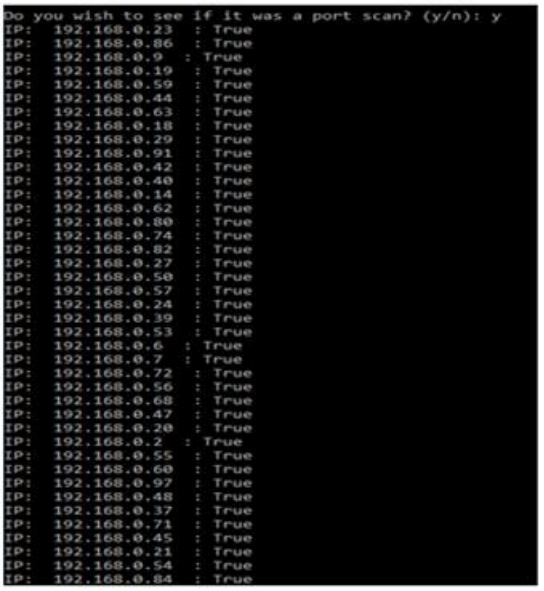

Fig.8: Evaluations the attacks done by the fictious node to different port numbers

V. CONCLUSION

In this paper ,discussing about the types of attacks and various detection techniques in OLSR routing protocol, Various definitions of the OLSR security is discussed, there are many Innovated isolated node detection techniques has been Proposed in the literature. However, the techniques almost concentrated on only a specific type of attack in OLSR routing protocol, the implementation of cost effective technique to handle multiple attacks in OLSR is appreciable. The distributed denial of service is an attack made by victims by entering into the website more than a time to cause damage to it. So to avoid this work helps to find who is login into the site every time by maintaining a Log Record. The Monitoring page will monitor the people who logins checks the time of login. If it is more than threshold value and it finds that it is hacker and blocks the person to log again. By using this we can save our system from the hackers within anorganization.

VI. FUTURE SCOPE

As the industry has been developingin a fast way, we can use the work in the network based system in the future. It will be useful to detect the hacker who uses the website.

VII. REFERENCES

[1]. Awerbuch, Baruch, and Amitabh Mishra. "Introduction to Ad hoc Networks."CS- 647: Advanced Topics in Wireless Networks, Department of Computer Science, John HupkinsUniversity(2008).
[2]. Djenouri, Djamel, L. Khelladi, and N. Badache. "A survey of security issues in mobile ad hoc networks." IEEE communications surveys7.4:2-28,2005.
[3]. He, Guoyou. "Destination-sequenced distance vector
[4]. (DSDV) protocol."Networking Laboratory, Helsinki University of Technology (2002):1-9.
[5]. Clausen, Thomas, and Philippe Jacquet. Optimized link state

routing protocol (OLSR). No. RFC3626.2003.

[6]. Jacquet, Philippe, et al. "Optimized link state routing protocol for ad hoc networks." Multi Topic Conference, 2001. IEEE INMIC 2001. Technology for the 21st Century. Proceedings. IEEE International.IEEE,2001.

[7]. Johnson, David B., David A. Maltz, and Josh Broch. "DSR: The dynamic source routing protocol for multi-hop wireless ad hoc networks." Ad hoc networking 5 (2001):139-172.

[8]. Chakeres, Ian D., and Elizabeth M. Belding-Royer. "AODV routing protocol implementation design." Distributed Computing Systems Workshops, 2004. Proceedings. 24th International Conference on. IEEE,2004.

[9]. Haas, Zygmunt J., Marc R. Pearlman, and Prince Samar. "The zone routing protocol (ZRP) for ad hocnetworks."(2002).

[10]. Ramasubramanian, Venugopalan, Zygmunt J. Haas, and EminGünSirer. "SHARP: A hybrid adaptive routing protocol for mobile ad hoc networks."Proceedings of the 4th ACM international symposium on Mobile ad hoc networking & computing.ACM,2003.

[11]. Dhillon,D.,Randhawa,T.S., Wang,M. and Lamont,L. "Implementing a Fully Distributed Certificate Authority in an OLSR MANET," IEEE WCNC2004, Atlanta, Georgia USA, March21-25,2004.

[12]. Yi, A. Adnane, S. David, and B. Parrein, "Multipath optimized link state routing for mobile ad hoc networks," Ad Hoc Networks, vol. 9, no. 1, pp. 28–47,2011.

[13]. Kannhavong, Bounpadith, et al. "A survey of routing attacks in mobile ad hoc networks."*IEEE Wireless Communications* 14.5:85-91.D,2007.

[14]. Raffo, C. Adjih, T. Clausen, and P. M€uhlethaler, "An advanced signature system for OLSR," in Proc. 2nd ACM Workshop Security Ad Hoc Sensor Netw, pp.10–16,2004.