ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

Mitigating Different Attacks in OLSR Protocol –A Survey

L.M.Mary Jelba[1], S.Gomathi[2]

Research Scholar, Dept. of Computer Science, Sri Krishna Arts & Science College Coimbatore, Coimbatore, Tamil Nadu, India[1]

Head of the Department, Dept. of Computer Technology, Sri Krishna Arts & Science College Coimbatore, Coimbatore, Tamil Nadu, India[2]

ABSTRACT: Wireless network utilize the node mobility and opportunistic contact among nodes for data communication, because the network structure infrastructure less. Due to this nature, many types of security threads affect Ad-hoc network process and performance. In this survey, we focused on different types of attacks and its mitigation strategy over ad-hoc network. In the infrastructure free network, the abnormal ad suspicious behavior of nodes affects the overall performance of the network. In this paper, we surveyed various techniques and methods used to mitigate different types of attacks and security threads in OLSR protocol. In this paper overview of OLSR, features of OLSR along with the attack detection and mitigation techniques comparisons are made.

KEYWORDS: Mobile ad-hoc networks, OLSR, security, DOS attack.

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 [1]. 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. In MANET, cooperative structure has been followed, this types of networking provides cost effective services. The cooperation on these networks is always based on contacts. 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 issues [2] 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. In the case of proactive which is also known as table-driven protocol, for example, DSDV [3] and OLSR [4], [5], each 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) [6] and AODV (Ad hoc On Demand Distance Vector) [7]. 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) [8] and Zone-based Hierarchal Link State routing protocol (ZHLS) [9], these are the popular hybrid protocols available in MANET.

DOI: 10.15680/IJIRCCE.2016. 0406209

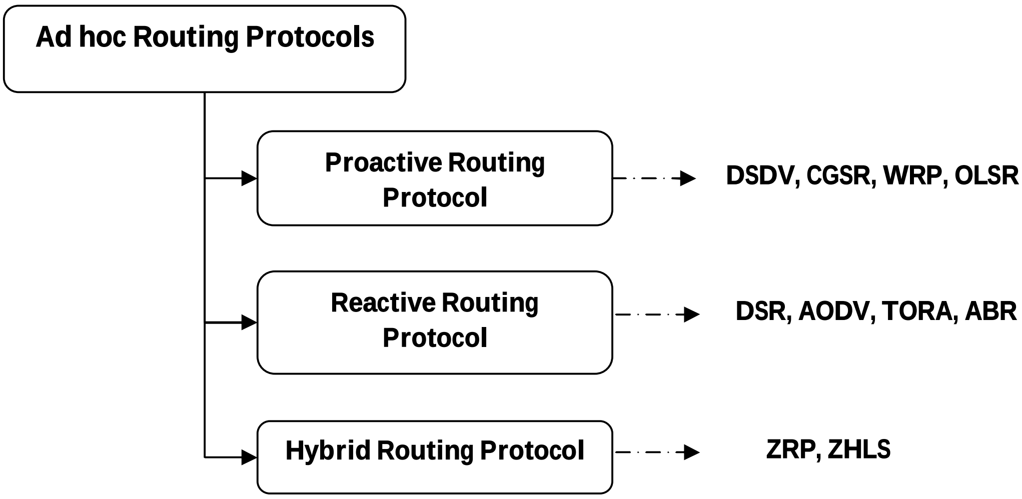

Fig 1.0 Types of ad hoc routing protocols

In this survey, we have concentrated on OLSR protocol and security issues over it. Several researches conducted many mitigation techniques against different attacks on different protocols in MANET. But only few researches concentrated on OLSR protocol, which has more unsecured control messages.

OLSR Protocol:

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 the neighborhood 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 sent periodically and the delivery does not have to be sequential.

The OLSR is easy to integrate with existing operating systems and it only interacts with the host routing table. This is more suitable for the application, which needs fast data transmission of the data packets with low delay.

The main process of OLSR is as follows.

- Neighbor sensing
- MPR (Multi Point Relay) selection
- MPR information declaration
- Route table calculation.

The main drawback of OLSR is it needs more time to rediscover a broken link. And it also needs more processing power at the time alternate route discovery.

With the security constraint, in OLSR all the control messages are needed to be secured. And the host and gateways are statically configured in order to advertise the routes to the valid addresses.

II. LITERATURE STUDY

In this section, we discuss security issues of the OLSR in various circumstances, i.e., at the time of route establishment, link discovery and data transmission. Attacks on the OLSR can be segregated into two types, such as passive and active attacks. In MANET a passive attack attains network transacted data without disturbing communications, whereas an active attack involves information interruption, disturbance, modification or fabrication which disrupts normal MANET process. Active attacks examples include jamming, impersonating, modification, Denial of Service (DoS) and message replay (wormhole attack).

Attacks in OLSR:

a. WORMHOLE ATTACK

Wormhole attack is the most common of attacks. It records traffic from one network region and replays it in another region. It is launched by an intruder node ‘X’ being within transmission range of legitimate nodes “Node A” and ‘Node B’, where ‘Node A’ and ‘Node B’ are not within transmission range of each other. The intruder ‘X’ node just routes control traffic between ‘Node A’ and ‘Node B’ and vice versa, without the modification accepted by the routing protocol.

i. Wormhole Attack in OLSR

As a wormhole attack can affect topology construction greatly, it is dangerous for many ad-hoc routing protocols, specially proactive routing protocols like OLSR, which exchange control packets for neighbor discovery/topology construction regularly.

Dhillon et al [10], proposed a Public Key Infrastructure (PKI) to improve security in a MANET running on OLSR routing protocol using a fully distributed Certificate Authority (CA). The proposed solution improves the control traffic load compared to using a centralized CA. However malicious nodes with proper credentials could not be identified.

Chriqi et al [11]. proposed the Secure Clustering based OLSR (SCOLSR). The main goal of their research was to increase the life time of ad-hoc networks in the presence of selfish nodes in the netwrok. The proposed algorithm effectively reduced the percentage of Multi Point Relay (MPR) nodes and thus reducing the traffic operating cost. It provided a mechanism to select cluster heads and MPR nodes based on the residual energy and the connectivity index. The proposed incentive mechanism was able to motivate nodes to cooperate under the threat that better network services will be provided only on accumulation of reputation.

Suresh et al [12], investigated collusion attack in MANET based on OLSR. They proposed a method Forced MPR S witching (FMS-OLSR) which observes symptoms of attack and temporarily blacklist potential attackers. Once blacklisted, the algorithm forces re-computation of its MPR set thus avoiding attacks.

Wang and Lamont [13], describe security threats to the OLSR MANET routing protocol. A semantic based intrusion detection solution was unfilled. The semantics properties are based on semantic properties implied in the OLSR routing behavior. However, the several existing solution did not address conflicts resolution and verification procedure for intruders.

Capkun et al [14] used directional antennas to prevent wormhole attacks. Each network node shares a secret key with each other and then broadcasts HELLO messages to discover neighbors through use of bi-directional antennas. SECTOR protocol suggested countermeasures against wormhole attacks include allowing nodes to prove their encounters with other nodes. But it requires several hypotheses for this protocol to work efficiently. These include the necessity for coarse synchronization, node ability to measure local timing with nanosecond precision, pre-establishment of security associations between pairs of nodes, and the central authority controlling network membership.

Babu et al [15], investigate the collusion attack in a MANET using OLSR protocol. During the presence of collusion attack the Packet Delivery Ratio (PDR) falls to zero percentage on the targeted node. In order to solve this issue, OLSR was enhanced by adding two new messages such as Trust REQuest (TREQ) and Trust REPly (TREP). Implementation of these additional control overheads was able to detect collusion attack and subsequently improved the PDP. The proposed improvement on OLSR does not require time synchronization or location improvement.

Hu et al [16] took recourse to packet leashes in a bid to protect reactive routing protocols against wormhole attacks. A leash is any information appended to a packet to reduce a packet’s maximum transmission distance. Two kinds of leashes are proposed: geographical and temporal leashes. In the former, the sender appends to a packet both sending time and location. Based on this, the receiving node computes an upper bound on the sender’s distance. This solution needs correct location information and network node synchronization. In temporal leash, the sender appends sending time to a packet while the receiving node computes the packet’s travelling distance assuming propagation at the speed of light, using the difference between packet's sending and receiving times. This solution needs a fine-grained synchronization between nodes.

Kahnnhavong et al [17], proposed a unique acknowledgement between two hop neighbors whenever the control traffic is successfully received. The proposed methodology was able to protect the network from link spoofing, wormhole attack without requiring location information or the full topology of the network. The proposed system was able to achieve higher packet delivery ratio compared to standard OLSR.

b. Node Isolation Attack

Another type of security attack in OLSR is Node isolation attack, which can results in denial-of-service (DOS) 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 [18], Nakayama et al. proposed a Denial of Service (DOS) attack against OLSR called node isolation attack. In this attack, an attacker exploits the fact that the victim prefers a minimal MPR set in order to hide the existence of the victim in the network. The attacker, which must be located within broadcast distance of the victim, advertises a fake HELLO message claiming to be in close proximity to all of the victim's two-hop neighbors. In addition, a fictitious node is advertised, giving the attacker an advantage over other possible legitimate candidates for MPR selection. Knowledge of the victim's two-hop neighbors is readily available by analyzing TC messages of the victim's one-hop neighbors, a list of which can be constructed directly from the HELLO message broadcast by the victim himself. MPR selection rules would cause the victim to exclusively select the attacker as its sole MPR, as it is the minimal set that allows for coverage of all of the victim's two-hop neighbors (including the fictitious node).

DOS is now straightforward. The attacker can isolate the victim simply by not including the victim in its TC message. In essence, the attacker refrains from notifying the network that the victim can be reached through it, and because no other node advertises a path to the victim, it is isolated.

Raffo et al. [19] 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. 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 network increases. Another problem is the fact that the network loses its spontaneity as all nodes are required to know each other in advance in order to share their public keys. This prevents the network from evolving naturally from the various nodes that appear at a certain place and time, a fundamental trait of MANETs. Another approach, based on local detection of link spoofing, is given by [20]. The authors provide a number of rules to identify abnormal behavior on the network. The solution includes a message sent in response to the detection of an intrusion, allowing for the exclusion of compromised nodes and preventing them from being included in network-wide routing tables. Besides the limited scope of the solution, as identification effectiveness is constrained to local nodes only, the ability of sending a warning message is disastrous in itself. Any malicious node can falsely advertise that some other node, local or remote, is malicious, causing for its immediate removal from routing tables all around. In a sense, the solution opens up an attack vector not present in the original problem.

III. CONCLUSION

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. In this survey, the above stated points are the main objective. The followings are the overall summary of the review by different metrics and parameters. In this survey research, we have discussed 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.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

REFERENCES

1. Awerbuch, Baruch, and Amitabh Mishra. "Introduction to Ad hoc Networks."*CS-647: Advanced Topics in Wireless Networks, Department of Computer Science, John Hupkins University* (2008).
2. Djenouri, Djamel, L. Khelladi, and N. Badache. "A survey of security issues in mobile ad hoc networks." *IEEE communications surveys* 7.4 (2005): 2-28.
3. He, Guoyou. "Destination-sequenced distance vector (DSDV) protocol."*Networking Laboratory, Helsinki University of Technology* (2002): 1-9.
4. Clausen, Thomas, and Philippe Jacquet. *Optimized link state routing protocol (OLSR)*. No. RFC 3626. 2003.
5. 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.
6. 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.
7. 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.
8. Haas, Zygmunt J., Marc R. Pearlman, and Prince Samar. "The zone routing protocol (ZRP) for ad hoc networks." (2002).
9. Ramasubramanian, Venugopalan, Zygmunt J. Haas, and Emin Gün Sirer. "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.
10. 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, March 21-25, 2004
11. . Chriqi, A., Otrok, H. and Robert, J-M. “SC-OLSR: Secure Clustering-Based OLSR Model for Ad-hoc Networks” IEEE International Conference on Wireless and Mobile Computing, Networking and Communications. page 239- 245, 2009.
12. Suresh,P.L, Kaur,R., Gaur M.S. andLaxmi V, “Collusion attack resistance through forced MPR switching in OLSR. IFIP Wireless Days. Page 1.2010.
13. Wang, M. and Lamont, L. “An Effective Intrusion Detection Approach for OLSR MANET Protocol.First IEEE ICNP Workshop on Secure Network Protocols, Page 55. 2005.
14. Capkun,S.,Buttyan,L. and Hubaux,J. “SECTOR: Secure Tracking of Node Encounters in Multi-hop Wireless Networks,” In Proc. ACM Workshop on Security of Ad-hoc and Sensor Networks (ACM SASN), Fairfax, USA, Oct. 2003
15. Babu, M.N.K., Franklin, A.A. and Murthy, C.S.R. “On the prevention of collusion attack in OLSR-based Mobile Ad-hoc Networks”. 16th IEEE International Conference on Network, page 1,2008
16. Hu, Y-C., Perrig, A. and Johnson, D. B. “Wormhole Attacks in Wireless networks”, IEEE Journal on Selected Areas in Communications, Vol. 24, No. 2, Pages: 370-380, 2006.
17. Kannhavong, Bounpadith, et al. "A survey of routing attacks in mobile ad hoc networks." *IEEE Wireless Communications* 14.5 (2007): 85-91.
18. B. Kannhavong, H. Nakayama, N. Kato, Y. Nemoto, and A. Jamalipour, “Analysis of the node solation attack against olsrbased mobile ad hoc networks,” in Proc. Int. Symp. Comput. Netw., 2006, pp. 30–35.
19. D. 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., 2004, pp. 10–16.
20. M. Wang, L. Lamont, P. Mason, and M. Gorlatova, “An effective intrusion detection approach for olsr manet protocol,” in Proc. 1st IEEE ICNP Workshop Secure Netw. Protocols, Nov. 2005, pp. 55–60.

DOI: 10.15680/IJIRCCE.2016. 0406209