Volume No:3, Issue No:4 (September-2017) ISSN No : 2454-423X (Online)

International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

OLSR Protocol Using Spears Contracts to Release Service Attacks

Krishna Priya Pingula
M.Tech Student,
Department of Computer Science and Engineering,
Christu Jyothi Institute of Technology & Science,
Jangaon.

A.Poorna Chandra Reddy
Associate Professor,
Department of Computer Science and Engineering,
Christu Jyothi Institute of Technology & Science,
Jangaon.

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. Over the years, emphasis has also been placed on improving the security of these networks. 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 who is able to isolate the victim from the rest of the network and subsequently deny communication services to the victim. In this paper, we suggest a novel solution to defend the OLSR protocol from node isolation attack by employing the same tactics used by the attack itself. Through extensive experimentation, we demonstrate that 1) the proposed protection prevents more than 95 percent of attacks, and 2) the overhead required drastically decreases as the network size increases until it is non-discernable. Last, we suggest that this type of solution can be extended to other similar DOS attacks on OLSR.

1. INTRODUCTION

A Mobile Ad Hoc Network (MANET) is a group of mobile devices capable of communicating wirelessly with each other without using a predefined infrastructure or centralized authority . Sending packets from one device to another is done via a chain of intermediate nodes. A number of different routing algorithms exist for network packet transmission. For the most part these algorithms can be classified into two main categories: reactive routing and proactive routing protocols. In the case of proactive (table-driven) protocol, for example, DSDV and OLSR every node constantly maintains a list of all possible destinations in the network and the optimal paths routing to it. Reactive protocols, such as DSR and AODV , find a route only on demand. Irrespective of routing algorithm, one of MANET's essential requirements of and a factor in its success is its ability of having all nodes recognized by other participants, even in motion. 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. Of the routing protocols mentioned above a proactive algorithm, the Optimized Link State Routing (OLSR) protocol has become one of the algorithms widely used today . Although OLSR is quite efficient in bandwidth utilization and in path calculation, it is vulnerable to various attacks. As OLSR relies on the cooperation between network nodes, it is susceptible to a few colluding rogue nodes, and in some cases even a single malicious node can cause routing havoc. These attacks include link withholding attacks , link spoofing attacks.

2. RELATED WORK

Service Provider:

In this module, the Service Provider browses the required file, initializes nodes with digital signature and uploads to the end user (node a, node b, node c, node d, node e, node f) via Router.

Router:

The Router is responsible for forwarding the data file in shortest distance to the destination; the Router consists of Group of nodes, the each and every node (n1, n2, n3,n4,n5,n6,n7,n8,n8,n10,n11,n12, n13) consist of Bandwidth and Digital Signature. If router had found any malicious or traffic node in the router then it forwards to the IDS Manager.

In Router we can assign the bandwidth for the nodes and can view the node details with their tags Node Name, Sender IP, Injected data, Digital Signature, Bandwidth and status.

IDS Manger(OLS Protocol):

The IDS manager is nothing but Intrusion Detection System manager which is responsible to filter the malicious data and traffic data. The IDS manager decides the phases based on Router status and then decides on two phases i.e., the “Training Phase” and the “Test Phase”.

Training Phase:

The Normal Profile Generation module is operated in the Training Phase to generate profiles for various types of legitimate traffic records, and the generated normal profiles are stored in a database.

Test Phase:

The Tested Profile Generation module is used in the Test Phase to build profiles for individual observed traffic records. Then, the tested profiles are handed over to the Attack Detection module, which compares the individual tested profiles with the respective stored normal profiles.

End User:

In this module, the End user can receive the data file from the Service Provider which is sent via Router, if malicious or traffic node is found in the router then it forwards to the IDS Manager to filter the content and adds to the attacker profile.

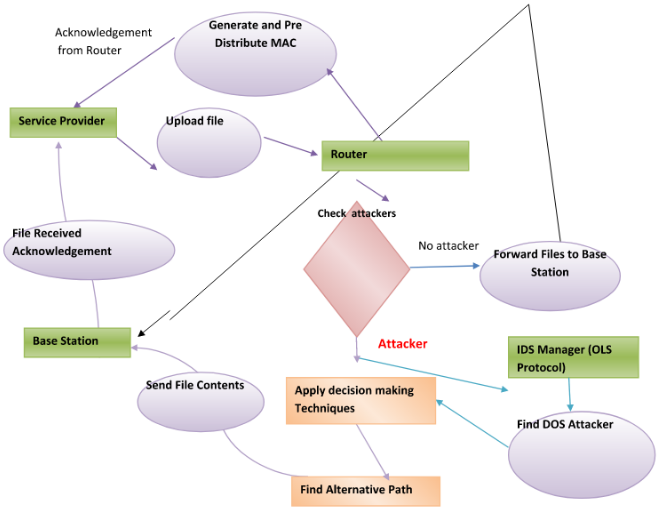
Forgery Attacker and DOS Attacker:

In this module, the malicious node or the traffic node details can be identified by a threshold-based classifier is employed in the Attack Detection module to distinguish DoS attacks from legitimate traffic.The Attacker can inject the fake message and generates the signature to a particular node in the router with the help of threshold-based classifier in testing phase and then adds to the attacker profile.

3. BACKGROUND

In the existing system, every node inspect its MPRs’ TC messages to see whether it has been included. This is possible due to the nature of the broadcast channel in wireless networks and also because MPR selection rules exclusively allow for the designation of MPRs within broadcast distance only. The existing system can conclude whether x is malicious by looking for its own address in x’s TC message; its lack thereof can only be due to malicious intent. This solution is elegant, but it has a number of drawbacks. First, this scheme is only effective against a single attacker, but, as the authors note, it fails in situations involving two consecutive colluding attackers. By having the first attacker orchestrates the attack yet advertise the correct TC, the victim cannot tell that it is under attack. The second colluding attacker, designated as the first’s sole MPR, removes the victim from the advertised TC prior to propagation, isolating it from the network. In the existing system, the system reviews a specific DOS attack called node isolation attack and proposes a new mitigation method. 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 network size increases, which is consistent with [4]’s general claim that OLSR functions best on large networks.

4. SYSTEM FLOW


Acknowledgement from Router
Generate and Pre Distribute MAC
Service Provider
Upload file
Router
Check attackers
No attacker
Forward Files to Base Station
File Received Acknowledgement
Base Station
Attacker
IDS Manager (OLS Protocol)
Send File Contents
Apply decision making Techniques
Find DOS Attacker
Find Alternative Path

5. CONCLUSION

In this paper, we have presented a solution called DCFM whose function is to prevent a node isolation attack in which the attacker manipulates the victim into appointing the attacker as a sole MPR, giving the attacker control over the communication channel. We further strengthened the attack by giving the attacker the ability to follow the victim around. DCFM is unique in that all the information used to protect the MANET stems from the victim's internal knowledge, without the need to rely on a trusted third party. In addition, the same technique used for the attack is exploited in order to provide protection. By learning local topology and advertising fictitious nodes, a node is able to deduce suspect nodes and refrain from nominating them as a sole MPR, thus, side-stepping the essential element of the attack. Simulation shows that DCFM successfully prevents the attack, specifically in the realistic scenario in which all nodes in the network are mobile. In addition, it was discovered that as node population increases in density and size, the closer DCFM overhead is to OLSR. Given that OLSR functions best in dense large networks, DCFM can function without real additional cost. We expect that with only minor adjustments, DCFM can protect OLSR from the family of attacks that centers around the falsification of HELLO messages with the intention of being appointed as sole MPR (e.g., black hole [7], gray hole [32], and wormhole [13] attacks). We leave this for future work. We also leave to further research the exact values of FICTITIOUS_CHECK_INTERVAL that minimize the overall computation but still leave mitigation active and responsive.

REFERENCES

[1] S. Mclaughlin, D. Laurenson, and Y. Tan, "Mobile ad-hoc network." (Aug. 10 2006) uS Patent App. 11/351,777. [Online]. Available: http://www.google.com/patents/US20060176829

[2] C. E. Perkins and P. Bhagwat, "Highly dynamic destinationsequenced distance-vector routing (dsdv) for mobile computers," in Proc. Conf. Commun. Archit., Protocols Appl., 1994, pp. 234–244.

[3] P. Jacquet, P. Muhlethaler, T. Clausen, A. Laouiti, A. Qayyum, and L. Viennot, "Optimized link state routing protocol for ad hoc networks," in Proc. IEEE Int. Multi Topic Conf. Technol., 2001, pp. 62–68.

[4] 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

[5] D. Johnson, Y. Hu, and D. Maltz, "Rfc: 4728," Dynamic Source Routing Protocol (DSR) Mobile Ad Hoc Netw. IPV4, 2007. [Online]. Available: http://tools.ietf.org/html/rfc4728

[6] C. Perkins and E. Royer "Ad-hoc on-demand distance vector routing," in Proc. 2nd IEEE Workshop Mobile Comput. Syst. Appl., Feb. 1999, pp. 90–100.

[7] E. Gerhards-Padilla, N. Aschenbruck, P. Martini, M. Jahnke, and J. Tolle, "Detecting black hole attacks in tactical manets using topology graphs," in Proc. 32nd IEEE Conf. Local Comput. Netw., Oct. 2007, pp. 1043–1052.

[8] C. Adjih, T. Clausen, P. Jacquet, A. Laouiti, P. Muhlethaler, and D. Raffo, “Securing the olsr protocol,” in Proc. Med-Hoc-Net, 2003, pp. 25–27.

[9] B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato, and A. Jamalipour, “A survey of routing attacks in mobile ad hoc networks,” IEEE Wireless Commun., vol. 14, no. 5, pp. 85–91, Oct. 2007.

[10] D. Dhillon, J. Zhu, J. Richards, and T. Randhawa, “Implementation & evaluation of an ids to safeguard olsr integrity in manets,” in Proc. Int. Conf. Wireless Commun. Mobile Comput., 2006, pp. 45–50.

[11] 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.

[12] C. Adjih, D. Raffo, and P. M€uhlethaler, “Attacks against OLSR: Distributed key management for security,” in Proc. 2nd OLSR Interop/Workshop, Palaiseau, France, 2005.