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.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

Enhanced Routing in Mobile Adhoc Network against Denial of Service Attack

V.R.Nisha, S.Rajeswari

Student/M.E (CSE), Sri Shanmugha College Engineering & Technology, India[1]

AP/CSE, Sri Shanmugha College Engineering & Technology, India[2]

ABSTRACT*:* Recently, mobile ad hoc networks became a hot research topic among researchers due to their flexibility and independence of network infrastructures, such as base stations. Due to unique characteristics, such as dynamic network topology, limited bandwidth, and limited battery power, routing in a MANET is a particularly challenging task compared to a conventional network.Since MANET assumes a trusted environment for routing, security is a major issue. In this paper we analyze 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 and replay attack. Analyzing the attack, we propose a mechanism called Enhanced OLSR (EOLSR) protocol which is a trust based technique to secure the OLSR nodes against the attack. Our technique is capable of finding whether a node is advertising correct topology information or not by verifying its Hello packets, thus detecting node isolation attacks and including timestamp to avoid replay attack.

KEYWORDS*:* Ad hoc networks, denial-of-service (DOS) attack, node isolation attack, optimized link state routing (OLSR), routing protocols.

I. INTRODUCTION

A mobile ad hoc network (MANET) is a collection of mo- bile devices which are connected by wireless links without the use of any fixed infrastructures or centralized access points. In MANET, each node acts not only as a host but also as a router to forward messages for other nodes that are not within the same direct wireless transmission range. Each device in a MANET is free to move independently in any direction, and will there- fore change its links to other devices frequently. MANETs are much more vulnerable and are susceptible to various kinds of security attacks because of its cooperating environment. In the absence of a fixed infrastructure that establishes a line of defense by identifying and isolating non-trusted nodes, it is possible that the control messages generated by the routing protocols are corrupted or compromised thus affecting the performance of the network.

Routing protocols in MANET can be classified into two categories: reactive protocol and proactive protocol. In proactive routing protocols, all nodes need to maintain a consistent view of the network topology. When a network topology changes, respective updates must be propagated throughout the network to notify the change. In reactive routing protocols for mobile ad hoc networks, which are also called "on-demand" routing protocols, routing paths are searched for, when needed. Even though many research works had been carried out for routing attacks in MANET, most of it concentrated mainly on re- active routing protocols. Optimized link state routing (OLSR) routing protocol which is a proactive routing protocol offers promising performance in terms of bandwidth and traffic overhead but it does not 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. In this paper, we analyze a specific DOS attack called node isolation attack and propose a solution for it. Node isolation attack can be easily launched on OLSR after observing the net- work activity for a period of time. We propose a solution called enriched OLSR (EOLSR) that is based on verifying the hello packets coming from the node before selecting it as a multipoint relay (MPR) node for forwarding packets.

II. OLSR OVERVIEW

Optimized link state routing (OLSR) is one of the most important proactive routing protocols designed for MANET. It employs periodic exchange of messages to maintain topology information of the network at each node. The key concept of OLSR is the use of multipoint relay (MPR) to provide efficient flooding mechanism by reducing the number of transmissions required. Each node selects a set of its neighbor nodes as MPR. Only nodes selected as MPR nodes are responsible for advertising as well as forwarding topology information into the network. Fig. 1 illustrates a node broadcast its messages throughout the network using standard flooding where all neighbors relay message transmitted by the leftmost node and MPR flooding where only MPR nodes relay the message. The protocol is best suitable for large and dense network as the technique of MPRs works well in this context. A node selects MPRs from among its one hop neighbors with "symmetric", i.e., bi-directional, links. Therefore, selecting the route through MPRs automatically avoids the problems associated with data packet transfer over unidirectional links.

In OLSR protocol, two types of routing message are used, namely, HELLO message and TC message. A HELLO message is the message that is used for neighbor sensing and MPR se lection.

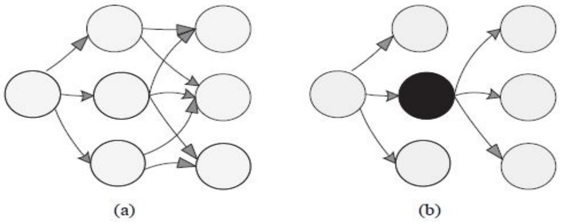

Fig. 1. Node broadcasting messages: (a) Regular flooding and (b) MPR flooding.

In OLSR, each node generates HELLO message periodically (every HELLO INTERVAL). A node's HELLO message contains its own address and the list its 1-hop neighbors. A TC message is the message that is used for route calculation. In OLSR, each MPR node advertises TC message periodically (every TC INTERVAL). A TC message contains the list of the sender's MPR selector. The protocol functioning of OLSR is as follows:

A. Neighbor Sensing

Neighborhood discovery is the process, whereby each router discovers the routers which are in direct communication range of itself (1-hop neighbors), and detects with which of these it can establish bi-directional communication. Each router sends HELLOs, listing the identifiers of all the routers from which it has recently received a HELLO, as well as the "status" of the link.

B.MRP Calculation

MPR Flooding is the process whereby each node is able to, efficiently, conduct network-wide broadcasts .Each router designates, from among its bi-directional neighbors, a subset (MPR set) such that a message transmitted by the router and relayed by the MPR set is received by all its 2-hop neighbors. Nodes may express, in their HELO messages, their "willingness" to be selected as MPR, which is taken into consideration for the MPR calculation. Each node selects its

MPR set from among its 1-hop neighbors such that they can reach all its 2-hop neighbors.

Each node maintains information about the set of neighbors 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.

C. Link State Advertisement

Link state advertisement is the process whereby routers are determining which link state information to advertise through the network. Each node must advertise, at least, all links between itself and its MPR-selector-set, in order to allow all nodes to calculate shortest paths. Such link state advertisements are carried in TCs, broadcast through the network using the MPR flooding process. As a node selects MPRs only from among

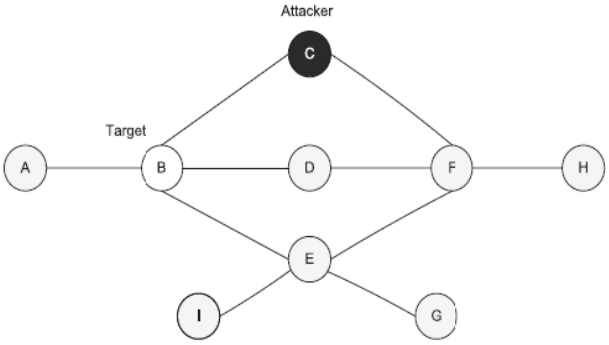

Fig. 2. Topology perceived by node H before the attack.

its bi-directional neighbors, links advertised in TC are also bi- directional and routing paths calculated by OLSR contain only bi-directional links. TCs are sent periodically, however certain events may trigger non-periodic TCs.

III. NODE ISOLATION ATTACK

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 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.

In this attack, attacker creates virtual links by sending fake HELLO messages including the address list of target node's 2- hop neighbors, (the attacker can learn victim's 2-hop neighbors by analyzing TC message of its 1-hop neighbors). According to OLSR protocol, the MPR selection is based on the maximum coverage of any node's 2-hop neighbors. 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 neighbors through the attacker it- self. Thus, the only node that must forward and generate TC messages for the target node is the attacking node. By drop- ping 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. 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 neighbors, 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.

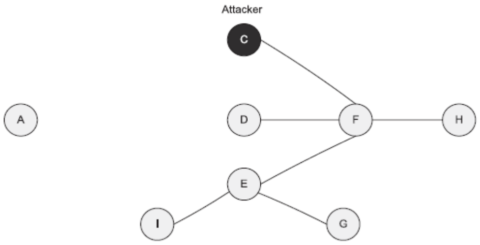

Fig. 3. Topology perceived by node H after the attack

In Fig. 2, node C is the attacking node, and node B is the tar- get node. Instead of sending correct HELLO message that contain {B, F} in neighbor address list, the attacker sends a fake HELLO message that contains {B, F, G, Z} which includes the target node's all 2-hop neighbors {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 neighbor 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 neighbor node Z can be reached only via node C (attacker) and all the other 2-hop neighbors 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. 3 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.REPLAY ATTACK

In a MANET, topology frequently changes due to node mobility. This means that current network topology might not exist in the future. In a replay attack [20], a node records another node's valid control messages and resends them later. This causes other nodes to record their routing table with stale routes. Replay attack can be misused to impersonate a specific node or simply to disturb the routing operation in a MANET.

A solution to protect a MANET from a replay attack by using a time stamp with the use of an asymmetric key. This solution prevents the replay attack by comparing the current time and time stamp contained in the received message. If the time stamp is too far from the current time, the message is judged to be suspicious and is rejected. Although this solution works well against the replay attack, it is still vulnerable to a wormhole attack where two colluding attackers use a high speed network to replay messages in a far-away location with almost no delay.

V. RELATED WORK

Recently, several cryptographic based techniques had been contributed for securing OLSR. A cryptographic based approach has been proposed for protecting the network. This technique classifies the OLSR nodes into either trusted or un-trusted nodes with an assumption that trusted nodes are not compromised. It integrates a timestamp and a signature with each routing control message: The signature is used to authenticate messages from trusted nodes, and timestamps are used to prevent replay attacks. The draw- back of this approach is that it does not deal with defense against compromised trusted nodes. But in our scheme, the hello packets generated by the authenticated nodes are also verified that enable us to detect the authenticated but compromised nodes.

The authors consider the compromise of trusted nodes. It is assumed that a public key infrastructure (PKI) and a timestamp algorithm are in place. Apart from routing control packets additionally this technique uses a message ADVSIG that contains time stamp and signature information. Each node maintains a table where information received in ADVSIGs is kept. Based on this information, each node verifies the correctness of the link state information in subsequent messages. The authors employed distributed key management techniques
to prevent wormhole and message replay attacks. The technique proposed in uses signature and timestamp schemes to en-sure authentication and protection against replay attacks. The techniques in imposes a large overhead to the network in terms of additional traffic and signature computations which results in high energy consumption at each node. Since our scheme does not depend on any encryption and decryption techniques, it does not add any computational complexity at each node.

A fully distributed certificate authority (CA) based on thresh- old cryptography is proposed in. In this technique a node can requests a certificate from any k nodes (shareholders) of the network that are authorized CAs. Each of the share holders determine whether to serve the request based on whether the node in question is well behaving. But this technique does not employ any monitoring system to determine the good behavior of network nodes, so that it does not deal with compromised trusted nodes.

The authors proposed a simple mechanism to detect the link withholding and misrelay launched by MPR nodes based on overhearing of traffic generated by 1-hop neighbors. But this technique requires promiscuous listening of neighbor nodes which result in energy drop at this node whereas we do not use any neighbor monitoring approach. proposed a cooperative security scheme using a complete path message (CPM) and rating table. This approach requires each node which receives a TC packet to send CPM back to the TC source. Based on the path information from the CPM, the TC source can detect the link spoofing attack. But this technique incurs a large overhead in terms of additional traffic, since it requires all nodes which receive TC message to generate a CPM message. Since CPM contains complete path it traversed, the size of the message increases as network grows. Our technique uses additionally three control messages which does not pass the network more than 3-hops, so that it does not incurs a large overhead in terms of traffic.

A formal approach to handle the MPR selection and defense against the security attacks in OLSR is suggested. This approach validates the routing table and the topology information using trust based reasoning. Hence, each node can verify the validity of the received HELLO and TC messages simply by correlating the information provided by these messages.

VI. CONCLUSION

This paper proposes a solution for node isolation attack launched against OLSR routing protocol. Here, we have discussed through an attack model, that it is easy for a malicious node to launch the node isolation attack and replay attack to isolate an OLSR MANET node. This attack allows at least one attacker to pre- vent a specific node from receiving data packets from other nodes that are more than two hops away. The proposed solution called EOLSR, which is based on OLSR, uses a simple verification scheme of hello packets coming from neighbor nodes to detect the malicious nodes in the network. Moreover, cooperative or colluding attack cannot be launched, because our technique doesn't employ any promiscuous listening of neighbor nodes for detecting the attackers.

REFERENCES

1. B. Kannhavong, H. Nakayama, and Jamalipour, "A survey of routing at- tacks in mobile ad hoc networks," IEEE trans. Wireless Commun., vol. 14, no. 5, pp. 85–91, Oct. 2007.
2. T. Clausen and P. Jacquet, "IETF RFC3626: Optimized link state routing protocol (OLSR),"Experimental,2003.
3. T.Clausen and U.Herberg, "Security issues in the optimized link state routing protocol version 2(OLSRv2)," Int. J. Netw. Security Appl., 2010.
4. B. Kannhavong, H. Nakayama and A. Jamalipour, "A study of routing attack in OLSR-based mobile adhoc networks," Int. J. Commun. Syst., 2007.
5. B. Kannhavong, H. Nakayama, N. Kato, Y. Nemoto, and A. Jamalipour, "Analysis of the node isolation attack against OLSR-based mobile ad hoc network," in Proc. ISCN, 2006, pp. 30–35.
6. D. Raffo, C. Adjih, T. Clausen, and P. Muhlethaler,"Securing the OLSR protocol," in Proc. Med-Hoc- Net, 2003.
7 . D. Raffo, C. Adjih, T. Clausen, and P. Muhlethaler, "An advanced signa- ture system for OLSR," in Proc. ACM SASN, 2004.
8. D. Raffo, C. Adjih, T. Clausen, and P. Muhlethaler "Attacks against OLSR: Distributed key management for security," in Proc. OLSR Interop and Workshop, 2005.
9. C. Adjih, T. Clausen, A. Laouiti, P. Muhlethaler, and D. Raffo, "Secur- ing the OLSR routing protocol with or without compromised nodes in the network," HIPERCOM Project, INRIA Rocquencourt, Tech. Rep. INRIA RR-5494, Feb. 2005.
10. D. Dhillon, T. S. Randhawa, M. Wang, and L. Lamont, "Implementing a fully distributed certificate autority in an OLSR MANET," in Proc. IEEE WCNC, 2004.
11 A. J. P. Vilela and J. Barros, "A cooperative security scheme for optimized link state routing in mobile ad-hoc networks," in Proc. IST MWCS, 2006.
12 A. Adnane, R. de Sousa, C. Bidan, and L. Mé, "Analysis of the implicit trust within the OLSR protocol," in Proc. IFIP, 2007.
13 X. Zeng, R. Bagrodia, and M. Gerla, "GloMoSim: A library for parallel simulation of large-scale wireless networks," in Proc. PADS, 1998.
14 D. Raffo, "Security schemes fo the OLSR protocol for ad hoc networks," Ph.D. dissertation,Univ. Paris, 2005
15 M. Mohanapriya and S. Urmila, "A novel technique for defending routing attacks in OLSRMANET,"inProc. IEEEICCIC,2010WCNC,2004.