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.5, Special Issue 2, April 2017
An International Conference on Recent Trends in IT Innovations - Tec'afe 2017
Organized by
Dept. of Computer Science, Garden City University, Bangalore-560049, India

Measuring Performance of OLSR and EOLSR during Routing Attack

Hamela K, Kathirvel Ayyaswamy

Research Scholar, Mother Teresa Women's University, Kodaikanal, India

Professor, Department of CSE, M.N.M. Jain Engineering College, Chennai, India

ABSTRACT: Optimized Link State Routing(OLSR) is a proactive routing protocol where each node maintains its routing information and get updated periodically. Some of the key features of OLSR are, it uses multi-relay point (MPR) for broadcasting routing information, it has controlled flooding mechanism, maintains minimum routing overhead and fast route discovery. OLSR is susceptible to various routing attack due to presence of fake nodes in the network topology which is the major drawbacks of this routing protocol. In our work we measure the performance of two routing protocol namely OLSR and EOLSR during routing attack. Three metrics like packet delivery, packet loss and control overhead are used to analyze these protocols during routing attack. We use NS2 as our simulator.

KEYWORDS: Enhanced Optimized Link State Routing(EOLSR); Node Isolation Attack; Optimized Link State Routing (OLSR),routing protocols

I. INTRODUCTION

Mobile adhoc network (MANET) is a wireless network with pre-define infrastructure. Since the nodes are dynamic in nature, the role of routing protocol is very much needed [5]. Routing protocol [5][13] is used to establish connection between nodes. Even the path establishment between source node and destination nodes can be accomplished by routing protocol. In MANET, Routing protocols are mainly classified into two types: proactive routing protocol and reactive routing protocol. In this paper, we will focus on one of the proactive routing protocol, namely OLSR, the concepts of OLSR uses link state protocol (LSP)[4]. A link state protocol has a feature of broadcasting information to all other nodes in the network topology. This feature will create multiple copies in each node again and again that result in flooding of data packets. The flooding of data packets can be controlled by using OLSR [4]. OLSR uses multi-point relay(MPR) to avoid repeated broadcasting of same data packets.

OLSR is also a table-driven protocol, where all network topology information are maintained by each node and it has to be updated periodically [3]. One of the major concerns of OLSR is prone to various routing protocol attack. In this paper we focus on, one type of routing attack namely Node Isolation attack. Node isolation attack in OLSR will isolate a normal node from the network topology with the help of malicious node. Because of these attacks, the performance of OLSR will reduce. To protect the node form the node isolation attack in OLSR, we consider another protocol known as enhanced optimized link state routing protocol(EOLSR)[12]. EOLSR uses the techniques of verifying the neighboring nodes with the concepts of trustworthiness [12]. In this paper we would like to measure the performance of OLSR and EOLSR during the node isolation attack. We would like to observe the performance of both the protocol during packet delivery ratio, packet lose ratio and control overhead.

The remaining part of the paper is organized as follows: Section II discusses the related work in the literature. Section III explains the concepts of OLSR. Section IV describes the node isolation attack in OLSR. The EOLSR is focused in Section IV. Section V shows the performance of OLSR and EOLSR. Section VI shows simulation result and we conclude in Section VII.

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.5, Special Issue 2, April 2017
An International Conference on Recent Trends in IT Innovations - Tec'afe 2017
Organized by
Dept. of Computer Science, Garden City University, Bangalore-560049, India

II. RELATED WORK

In this section, the work related to node isolation attack is being specified.
Balaji et al[14] , the author proposed a mechanism for securing the OLSR against node isolation attack. The methodology is capable of finding the correctness of information of hello message. The methodology was able to achieve in routing security towards increasing throughput, packet delivery frequency and control overhead.

N. Schweitzer et al [9], proposed a solution for node isolation attack called denial contradictions with fictitious node mechanism (DCFM). This proposal check for integrity between the HELLO message and the existing topology. The author claims that through this method he was able to prevent 95% of attacks and he claims that the overhead needed decreases as the network size increases.

Devesh et al[10] ,proposed a new methodology which can preserve energy with the help of modifying the original OLSR and also safe guarding the network form node isolation attack. The name specified for this proposal is denial of service free OLSR (DFOLSR).

III.OPTIMIZED LINK STATE ROUTING PROTOCOL

OLSR is a proactive routing protocol so that each node maintains routing information and it has to updated periodically[5]. OLSR hold two types of routing messages namely HELLO and TC messages. There are three way to perform routing operation in OLSR that include neighbor sensing, MPR selection and topology information.

A Neighbor Sensing

The feature of OLSR is to understand the neighboring information. To identify the neighbor node, the HELLO messages are send periodically in the network topology. These HELLO message are transmitted only to one-hop away. The HELLO message has to be broadcasted among the one-hop neighbor and routing table will get updated periodically. The main strategy of HELLO message, is to identify the one hop neighbor and also to select multipoint relay(MPR) nodes for broadcasting.

B. MPR Selection

MPR is used to control the flooding and also used to calculate shortest route between source node to destination node during packet transmission by using only selected nodes. Each node will select its own MPR. MPR selection required to choose minimum set of nodes from its neighbors, so that all its two hop neighbors will be included. Set of MPRs will be able to transmit to all two-hop neighbors. The link established between node & MPRs is bi-directional.

C Topology information

The MPR node will transmit TC message to entire network topology. TC messages are send to advertise its own link on the network. So that TC message is used as intra-forwarding database. TC messages are forwarded only by MPR nodes periodically. TC messages contain MPR selector, destination address, sequence number and holding time.

IV. NODE ISOLATION ATTACK IN OLSR

It is one type of Denial of service performed by malicious node, against the OLSR protocol [6]. The attacker node creates fake link information. The attacker node acts as if it has got maximum number of neighbor nodes, so that target node will select the attacker node as MPR. Once attacker node is selected as MPR, it allows the target node to communicate only with itself. The target node sends and receives information only to the attacker node. There by, making target node to be isolated from other nodes in network topology. This type of isolation of node is called node isolation attacks as shown in Figure 1.

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.5, Special Issue 2, April 2017
An International Conference on Recent Trends in IT Innovations - Tec'afe 2017
Organized by
Dept. of Computer Science, Garden City University, Bangalore-560049, India

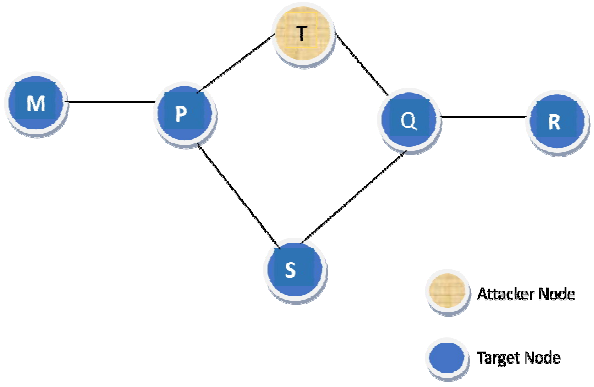

Fig 1 Network Structure with nodes M,P,Q,R,S,T

Assume node P is a target node, node T is an attacker node and we have other nodes like M,Q,R,S nodes available on the network. The attacker node T send false hello message to target node P. The target node P, will select the attacker node T as MPR, assuming that it has got many neighbour nodes with himself. After attacker node T is selected as MPR, the target node P will send and receive data packets only to attacker node T. And attacker node T will isolate target node P from all other nodes. There by target node P start dropping its data packets. At some period of time, node P will be totally isolated from other neighbour nodes. Since there won't be any communication from node P, the other nodes will consider node P as not in range. And node P will be isolated from other nodes, as shown in the figure.

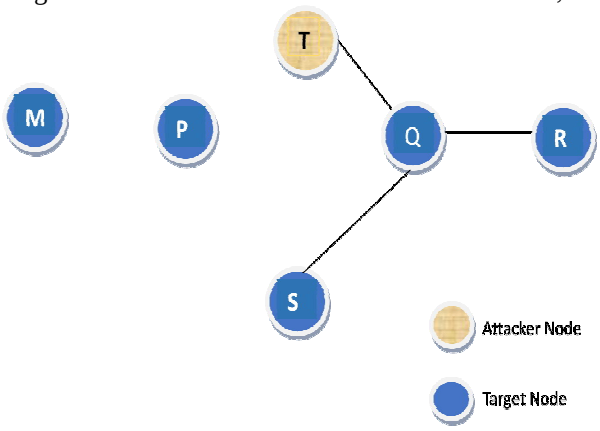

Fig 2 Network Structure after node isolation attack

V. EOLSR

EOLSR is an enhancement of the basic OLSR routing protocol that will be able to identify fake nodes in the network. The main goal of this proposal is to reject any fake node that will provide false information about any normal node. In this approach, authentication mechanism is used through which we can restrict the node from sending fake link address. The major contribution of this proposal is trustworthiness of HELLO messages to be verified by the neighbor node.

In EOLSR along with HELLO and TC messages, three more control packets are maintained like 2-hop request, 2-hop reply and node exist query(NEQ). If a new node sends HELLO message to an existing node, then the existing node updates its one-hop table containing new node information in it. After including new nodes it has to send a 2-hop request to neighboring node for checking the trustworthiness of new node. If new node presents in 2-hop reply, the current node selects a new node as its MPR. Otherwise, new node will be rejected and will be send to fake node list. Then the current node after receiving fake node information, broadcast to the entire network about fake node through

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.5, Special Issue 2, April 2017
An International Conference on Recent Trends in IT Innovations - Tec'afe 2017
Organized by
Dept. of Computer Science, Garden City University, Bangalore-560049, India

TC and HELLO messages. Through this precaution message, all nodes reject the entire fake node route and the fake node is removed from the routing table. Thus, a new MPR is selected only based on trust worthiness of the nodes, otherwise data forwarding will be continued using the existing MPR nodes itself.

VI. PERFORMANCE OF OLSR AND EOLSR

In this section effort has been made to measure the performance of OLSR and EOLSR through various strategies. Some of common key strategies of OLSR and EOLSR are:

a) Pro-active routing protocol

OLSR and EOLSR are proactive optimized link state protocol. Each node in the protocol maintains the routing information and it gets updated periodically. Due to proactive [5] in nature, OLSR and EOLSR will have low latency and high routing overhead.

b) Bandwidth Utilization

Bandwidth is the measure of number of packets send to final destination node per unit time. Each node in OLSR and EOLSR protocol get updated periodically which will result in high bandwidth utilization.

c) Link State Algorithm

OLSR and EOLSR uses link state algorithm, with controlled flooding. The control flooding is achieved because of MPR, which will select only few nodes for transmission. Broadcasting the same information again and again is avoided in both OLSR and EOLSR

d) No centralized control

In OLSR and EOLSR, no centralized control exists. Each node will forward the packets with the help of routing protocols.

e) Routing Structure

OLSR contains table driven routing structure that maintains HELLO and TC message tables. EOLSR also contains table driven routing structure, along with HELLO and TC message tables. This has to maintain three more control tables namely, 2-hop request, 2-hop reply, and node exist query(NEQ).

f) Security

OLSR has no security features built in it. It is vulnerable to various attacks like worm hole attack, link spoofing attack, node isolation attack. EOLSR contain security measure within itself. HELLO message will be verified by the neighbor node for checking the authentication of the node. This protocol can control node isolation attack.

VII. SIMULATION RESULT

The performance evaluation on the both OLSR and EOLSR technique during node isolation attack was conducted using network simulation NS2 [8]. Simulation settings and parameters are summarized in table 1.

Table 1
Simulation Setting

Parameters	Values
No. of Nodes	100
Area Size	1000 X 1000
Mac	802.11
Radio Range	250m
Simulation Time	10,20,30,40 and 50 sec
Routing Protocol	MOLSR

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.5, Special Issue 2, April 2017
An International Conference on Recent Trends in IT Innovations - Tec'afe 2017
Organized by
Dept. of Computer Science, Garden City University, Bangalore-560049, India

Traffic Source	CBR
Packet Size	512
Speed	5m/s

For performance evaluation of OLSR and EOLSR under node isolation attack are considered and result are shown in Fig. 3 and 4.

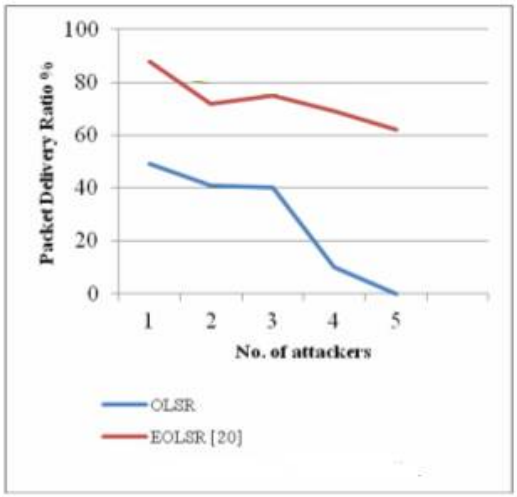

Fig 3. No. of attackers vs Packet delivery ratio

a. Packet delivery ratio: It is the ratio of the number of packets transmitted by the source nodes to the number of packets received by the destination nodes.

b. Packet loss rate: It is the number of data packets dropped by the fake nodes that are selected as MPR nodes.

c. *Control packet overhead*: This is the ratio of number of control packets to the data packet received.

Fig. 3 shows the measure the packet delivery ratio. We have considered attackers starting from 1 to 5 numbers. In OLSR, if fake node is selected as MPR, the MPR start dropping the packets as it receive and gradually decreases to zero, if number of attackers increased. In EOLSR, MPR packets start dropping the packet, if MPR is attacked by fake node, but due to its sustainable capacity dropping of packet didn't reach to zero level like OLSR.

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.5, Special Issue 2, April 2017
An International Conference on Recent Trends in IT Innovations - Tec'afe 2017
Organized by
Dept. of Computer Science, Garden City University, Bangalore-560049, India

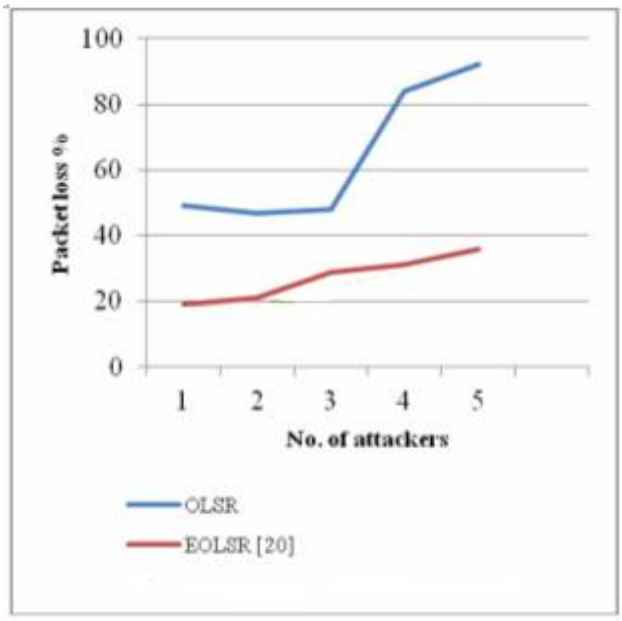

Fig 4 No. of attackers vs Packet loss ratio

Fig 4 shows the number of packets dropped by the fake nodes in OLSR and EOLSR. In case of OLSR, packet loss is more and but in EOLSR, which has a capacity to check for fake node before MPR selection, it was able to maintain stable packet lose.

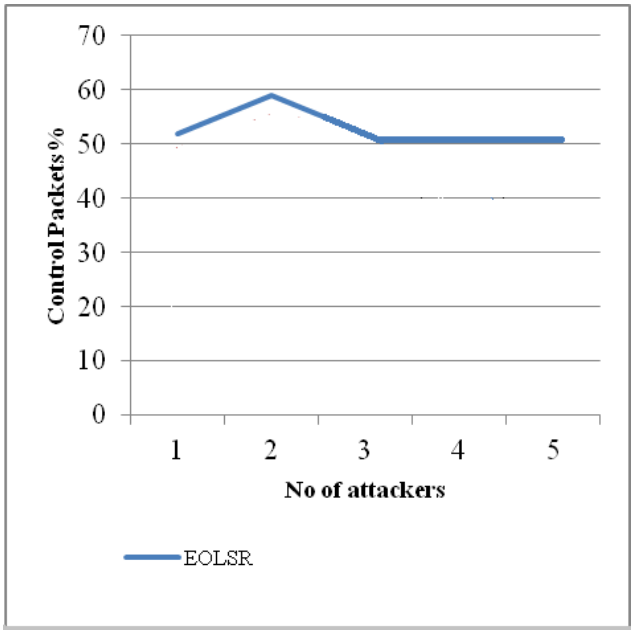

Fig 5 No. of attackers Vs Control packets

Fig 5 shows the number of attckers vs control packet ratio. EOLSR performs better in terms of control overhead as it is low compared to OLSR.

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.5, Special Issue 2, April 2017
An International Conference on Recent Trends in IT Innovations - Tec'afe 2017
Organized by
Dept. of Computer Science, Garden City University, Bangalore-560049, India

VIII. CONCLUSION

In this paper, we have measured the performance of OLSR and EOLSR during node isolation attack in MANET. OLSR has the capacity to control the flooding mechanism, but it fails to provide security for its network structure. These security aspects of OLSR can be overcome in our approach EOLSR. EOLSR selects MPR based on trustworthiness and verification, by which only the authenticated nodes can become MPR. Because of this, we were able to prevent this protocol from node isolation attack. We have implemented these model in NS2, considering the node isolation attack over the network structure. The two models were simulated in NS2 and result show that EOLSR outperforms OLSR in terms of security.

REFERENCES

[1] Ayyaswamy Kathirvel and Rengaramanujam Srinivasan, "ETUS: Enhanced Triple Umpiring System for Security and Robustness of Wireless Mobile Ad Hoc Networks", International Journal of Communication Networks and Distributed Systems, Vol. 7, No. 1 / 2, pp. 153 – 187, 2011.
[2] Ayyaswamy Kathirvel and Rengaramanujam Srinivasan, "ETUS: An Enhanced Triple Umpiring System for Security and Performance Improvement of Mobile Ad Hoc Networks", International Journal of Network Management, Vol. 21, No. 5, pp. 341 – 359, 2011.
[3] N.Kirubakaran and A.Kathirvel, "Performance Improvement of Security Attacks in wireless Mobile Adhoc Networks", Asian Journal of Information Technology, Vol. 13, No. 2, pp. 68 – 76, 2014.
[4] Loutfi ; M. Elkoutbi," Enhancing Performance OLSR In MANET", Multimedia Computing And Systems (ICMCS), 2012 ,DOI: 10.1109/ICMCS.2012.6320206 , IEEE
[5] Arefin, Khan and Toyoda, "Performance analysis of mobile ad-hoc network routing protocols", IEEE conference, May 2012, pp. 935-939
[6] Kannhavong ; H. Nakayama ; N. Kato ; Y. Nemoto ; A. Jamalipour," Analysis Of The Node Isolation Attack Against OLSR-Based Mobile Ad Hoc Networks", ,DOI: 10.1109/ISCN.2006.1662504 , IEEE
[7] K.UrmilaVidhya , M. MohanaPriya," A Novel Technique For Defending Routing Attacks In OlsrManet", 2010 IEEE International Conference On Computational Intelligence And Computing Research
[8] N.Kirubakaran and A.Kathirvel, "Performance Improvement of Security Attacks in wireless Mobile Adhoc Networks", Asian Journal of Information Technology, Vol. 13, No. 2, pp. 68 – 76, 2014.
[9] N. Schweitzer, A. Stulman, A. Shabtai and R. Margalit, "Mitigating Denial of Service Attacks in OLSR Protocol Using Fictitious Nodes", IEEE Transactions on Mobile Computing, vol. 15, no. 1, pp. 163-172, 2016.
[10] DeveshMalik,Krishna Mahajan,M.A.Rizvi,"Security for Node Isolation Attack on OLSR by Modifying MPR Selection Process",2014 First International Conference on Networks & Soft Computing
[11] Network simulator: http:///www.isi.edu/nsnam/ns.
[12] M. Marimuthu and I. Krishnamurthi, "Enhanced OLSR for defense against DOS attack in ad hoc networks", Journal of Communications and Networks, vol. 15, no. 1, pp. 31-37, 2013.
[13] Sheetal Sisodia, SandeepRaghwanshi, "Performance Evaluation of a Table Driven and On-Demand Routing Protocol in Energy Constraint MANETs", 2013 International Conference on Computer Communication and Informatics (ICCCI-2013), Jan. 04–06, 2013.
[14] Balaji S. Shivanakar; Sandeep A. Thorat,"Addressing node isolation attack in OLSR protocol", 2015 International Conference on Advances in Computing, Communications and Informatics (ICACCI)Pages: 1013 - 1019, DOI: 10.1109/ICACCI.2015.7275743