Identifying various Routing Attacks in Optimized Link State Protocol

Hamela K, Kathirvel Ayyaswamy

Abstract— A computer network which can be established without a predefined infrastructure is known as wireless adhoc network. Adhoc network can also be classified into various category like Mobile adhoc networks (MANETs),Vehicular ad hoc networks (VANETs),Smartphone ad hoc networks (SPANs),Internet-based mobile ad hoc networks (iMANETs), Military and Tactical MANETs. Here we discuss about one type of wireless adhoc network namely MANET. In MANET, each node itself acts as a router to communicate with neighboring nodes. For the purpose of establishing route between nodes we use routing protocols, which will help to transfer the data packets. Routing protocol in MANET is organized as pro-active routing protocol and reactive routing protocol. One type of pro-active routing protocol is Optimized Link State Protocol (OLSR). In this paper we try to identify various routing attacks in OLSR.

Index Terms— Attacks in OLSR, Link State Protocol, Mobile Adhoc Network, Optimised Link State Routing

1 INTRODUCTION

MOBILE Adhoc Network is a computer network which has to be setup without any infrastructure. The nodes in the network itself act as a router and launch the network connection. Other important aspects to be looked in MANET are nodes are mobile in nature, its lack in bandwidth availability, and also its faces hidden & exposed terminal problem. To construct a MANET with these limitations, we need a well-defined routing protocol, which can find a path between source node and destination node and also we need routing protocol to maintain route information of entire network. MANET are often used in Battlefield, emergency services were we cannot establish wired connection.

The working principal of routing protocol in MANET can be divided into proactive routing protocol and reactive routing protocol as shown in Figure 1. Reactive routing protocol, route information is exchanged between nodes when it wants to send packets to the destination node. These concepts otherwise called as On Demand routing protocols. Example: DSR, AODV. In proactive routing, a special table called routing table is maintained periodically by every node. This table will maintain all routing information of entire network. Proactive routing protocol, otherwise called as reactive routing protocol. Example: OLSR, FSR[9].

The remaining part of the paper is organized as follows. Section 2 gives the concepts of OLSR, Section 3 performance of OLSR, section 4 contribute towards the various routing attack against OLSR and we conclude with future work in section 5.

IJSER

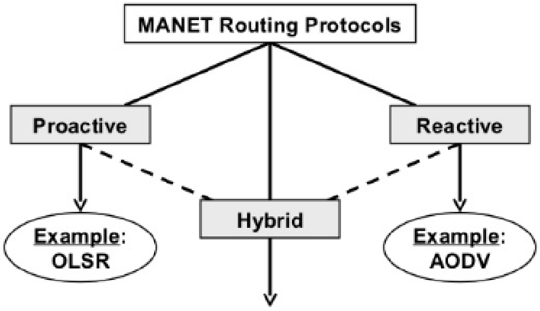

Fig 1 Types of MANET Routing Protocol

2 OPTIMIZED LINK STATE PROTOCOL

One of the proactive routing protocols is OLSR, which was designed based on link state protocols in Figure 2. Link state protocol(LST) uses traditional way of broadcasting all node information to all other nodes. The major drawbacks we face using link state protocol is node information had being send again and again, which tends to create multiple copies. But OLSR uses link state algorithm in optimized manner to overcome the drawbacks of LST.

- *Hamela K is currently pursuing Ph.d program in Mother Teresa Women's University and working as Assistant Professor, Department of Compter Science, Government First Grade College, Kolar Gold Field, India, E-mail:hamela27@gmail.com*
- *Kathirvel Ayyaswamy is a Professor at the Department of Computer Science Engineering of M.N.M Jain Engineering College, Chennai, India.*

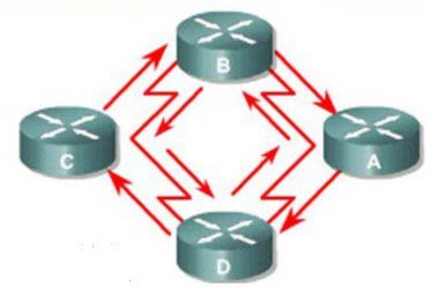

Fig 2 Link State Routing Protocol

OLSR uses multipoint relay (MPR) feature for calculating the shortest path between neighboring nodes. The flooding mechanism is maintained by MPR, so that it can avoid the repeated broadcasting. OLSR consists of two types of routing message namely HELLO message and TC message [6].

HELLO messages are periodically exchanged among neighboring nodes to find the status of the neighbor node. HELLO message will also maintain MPR selection details. It maintains a table called neighbor table, which consist of neighbor node status, and link status of the nodes namely unidirectional, bidirectional and multipoint relay. It can be send only to one hop network.

IJSER

Using TC messages, each node periodically broadcast TC message throughout the network. TC message used to send MPR selector list and MPR host will forward the TC message. The main activity of TC message is to send all topology information to the entire network structure.

Multiple Interface Declaration (MID) message is also maintained in OLSR. MID used to inform other nodes that the possibility of nodes participating in OLSR routing. MID are used to send information about all the nodes participating in the OLSR routing [7].

a. *Routing in OLSR*

Routing operation in OLSR can be performed using three way namely, neighbor sensing, MPR selector and Topology information.

Neighbor sensing

The major properties of link state protocol is the node should know the information about their neighbor. To recognize the neighbor node, the Hello messages will be sending periodically. These Hello message are transmitted only one hop away, so that hello message don't have permission to transmit further. The nodes send and receive broadcast message among neighbor and gets its information updated in routing table.

Hello message will help to understand the status of neighbor node and to identify the MPR nodes[11].

Multipoint relay

MPR is the key factor of OLSR, to avoid flooding of node information, MPR reduces the number of nodes broadcasting the information their by reducing information exchange overhead. Due to broadcasting of hello packet message periodically, each node will have one-hop and two hop neighbor information [9].

MPR selection algorithm

The two steps performed by MPR selection algorithm are discussed below. Consider each point u has to select its set of MPR. Here one-hop neighborhood is considered as (N1(u)) and two-hop neighborhood is considered as (N2(u)).

Step 1: Select the nodes of N1(u) which covers isolated points of n2(u).
Step 2: Select the nodes which was not selected in Step 1. Try to identify the node which covers highest number of points of (N2(u)) and continue on till every points of N2(u) are covered[4].

This MPR selection is most suitable for larger networks, through which we can avoid same packet being transmitted again and again.

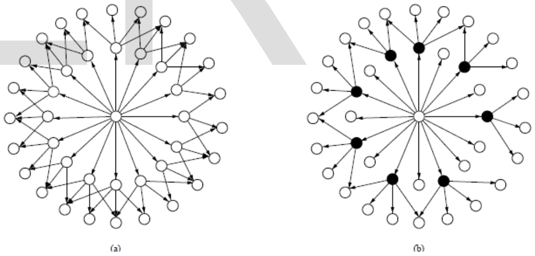

Fig. 3 Two hop neighbors and "multipoint relays" (the solid circles) of a node. (a) illustrates the situation where all neighbors retransmit a broadcast, (b) illustrates where only the MPRs of a node retransmit the broadcast

Topology information

The MPR node needs to transmit TC message. TC message is send to entire network and MPR only will give permission to forward TC message.TC message is sent by the node to advertise its own link in the network.

Routing table calculation

Since, it is a proactive in nature, routing table will maintain all routes for all nodes in the network structure. The routing table withholds information like destination address, next address, no. of hops to the destination node. To find the routes for the routing table shortest path algorithm is used.

3 Routing Attacks In Manet

Due to lack of centralized control and mobile nature of the nodes, OLSR tends to undergo various routing attacks. OLSR has to face various routing protocol attacks like worm hole attack, node isolation attack, link spoofing attack, denial of service attack, black hole attack, flooding attack, colluding mis-relay attack [1-3].

a. *WORM HOLE ATTACK*

The attackers try to combine one or more nodes at same location and re-route them to another location. This kind of attack normally targets the routing packets and re-reroute them to alternative remote location. Thus at one stage all router will be directed to wormhole which was established by the attackers. OLSR is always vulnerable to worm hole attack.

b. *NODE ISOLATION ATTACK*

It is one of the attacks which is suffered by OLSR. The main focus of the attack is to isolate node from communicating with other node. The isolated node will not be able to receive link information from the source node, due to which, the isolated node will not be able to send data to other nodes. This attack is carried out by targeting MPR selection algorithm [14].

IJSER

c. *LINK SPOOFING ATTACK*

This type or attack is carried out in Hello message & TC message transmission. Hello message spoofing attack can be achieved in three ways:

a. By adding fake node information
b. By adding false neighbor information
c. By deleting existing node information.

TC message spoofing can be carried out by adding fake MPR selector information and by deletion of MPR selector information [16].

d. *DENIAL OF SERVICE ATTACK*

Denial of service attacks target the resource utilization of nodes. Due to lack of resources, nodes will start acting greedy with other nodes in sharing resources [8]. Some of the resources targeted by DOS attack are

- Storage and Processing Resources
- Energy Resources
- Bandwidth

e. *COLLUSION ATTACK*

In collusion attack, two or more attackers join with each other to perform the attack in order to interrupt routing operation in OLSR.

f. *BLACK HOLE ATTACK*

Nodes which act as black hole send wrong hello messages. This black hole node project themselves as nodes with more links to its neighbors. By which, black hole node will be selected as MPR node. There by black hole node will target for TC message and try to capture the route of the network structure [15].

IV CONCLUSION

A MANET is organized as a group of mobile nodes which has no fixed infrastructure and also it lack in centralized control. Routing protocol plays a vital role in making the information to transmit from source node to destination node. In this paper, we focused on one type of routing protocol namely OLSR. OLSR has characteristic to update information periodically and also it maintains node information in routing table. Since the nodes are mobile in nature and periodic update of routing information required. OLSR has to face various security issues. We have discussed about various routing attack in OLSR. In future we will try to find a mechanism to overcome the routing attack in OLSR.

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] Mr. K.Prabu, Dr. A.Subramani,” Performance Analysis Of Modified OLSR Protocol

[5] For MANET Using ESPR Algorithm”, ICICES2014 - S.A.Engineering College, Chennai, Tamil Nadu, Indiaisbn No.978-1-4799-3834-6/14/$31.00©2014 IEEE

[6] Mahmood Salehi ; Hamed Samavati ; Mehdi Dehghan,”Performance Assessment Of OLSR Protocol Under Routing Attacks, In: *Internet Technology And Secured Transactions*”, ICITST), 2011 International Conference ,IEEE Xplore: 09 February 2012,INSPEC Accession Number: 12540161, IEEE

[7] P. Jacquet, P. Muhlethaler, T. Clausen, A. Laouiti, A. Qayyum And L. Viennot, "Optimized Link State Routing Protocol For Ad Hoc Networks," *Multi Topic Conference, 2001. IEEE INMIC 2001. Technologyfor The 21st Century. Proceedings. IEEE International*, 2001, Pp. 62-68. Doi: 10.1109/INMIC.2001.995315

[8] Loutfi ; M. Elkoutbi,” Enhancing Performance OLSR In MANET”, *Multimedia Computing And Systems (ICMCS)*, 2012 ,DOI: 10.1109/ICMCS.2012.6320206 , IEEE

[9] Mohanapriya Marimuthu And Ilango Krishnamurthi,” Enhanced OLSR For Defense Against DOS Attack Inad Hoc Networks”, *Journal Of Communications And Networks*, Vol. 15, No. 1, February 2013

[10] Basu Dev Shivahare ,Charu Wahi , Shalini Shivhare,” Comparison Of Proactive And Reactive Routing Protocols In Mobile Adhoc Network

Using Routing Protocol Property, *International Journal Of Emerging Technology And Advanced Engineering*, ISSN 2250-2459, Volume 2, Issue 3, March 2012)

[11] Gagandeep, Aashima, Pawan Kumar," Analysis Of Different Security Attacks In Manets On Protocol Stack A-Review" *International Journal Of Engineering And Advanced Technology* (IJEAT)ISSN: 2249 – 8958, Volume-1, Issue-5, June 2012 269

[12] Aleksandr Huhtonen, "Comparing AODV And OLSR Routing Protocols", *Helsinki University Of Technology, Telecommunication Software And Multimedia Laboratory.*

[13] Bounpadith Kannhavong , Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, Yoshiaki Nemoto," A Study Of A Routing Attack In OLSR Based Mobile Ad Hoc Networks ", *International Journal Of Communication Systems*,14 March 2007 DOI: 10.1002/Dac.870

[14] K.Urmila Vidhya , M. Mohana Priya," A Novel Technique For Defending Routing Attacks In Olsr Manet", 2010 *IEEE International Conference On Computational Intelligence And Computing Research*

[15] B. Kannhavong ; H. Nakayama ; N. Kato ; Y. Nemoto ; A. Jamalipour," Analysis Of The Node Isolation Attack Against OLSR-Based Mobile Ad Hoc Networks", Date Of Conference: 16-18 June 2006,DOI: 10.1109/ISCN.2006.1662504 , *IEEE*

[16] Bounpadith Kannhavong, Hidehisa Nakayama1, Nei Kato1, Abbas Jamalipour And Yoshiaki Nemoto," A Study Of A Routing Attack In OLSR-Based Mobile Ad Hoc Networks", Published Online 14 March 2007 In Wiley *Interscience (Www.Interscience.Wiley.Com*). DOI: 10.1002/Dac.870

[17] Yuseok Jeon, Tae-Hyung Kim," LT-OLSR: Attack-Tolerant OLSR Against Link Spoofing" *Division Of IT Convergence Engineering, 37th Annual IEEE Conference On Local Computer Networks* LCN 2012, Clearwater, Florida.

[18] .M.P. Martinez, R.B. Llavori, M.J.A. Cabo, and T.B. Pedersen, "Integrating Data Warehouses with Web Data: A Survey," *IEEE Trans. Knowledge and Data Eng., preprint,* 21 Dec. 2007, doi:10.1109/TKDE.2007.190746.(PrePrint)

IJSER