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. 3, Issue 11, November 2015

Methods to prevent flooding disruption in Optimized Link State Routing (OLSR) Protocol: A survey

Jigna Bavaliya, Prof. Rashmi Agrawal, Prof.Archana Gondaliya

M.E. Student, Dept. of Computer, Atmiya Institute of Technology and Science, Rajkot, India

Training & Placement Officer, Dept. of CE, Atmiya Institute of Technology and Science, Rajkot, India

Assistant Professor, Dept. of CE, Atmiya Institute of Technology and Science, Rajkot, India

ABSTRACT: MANET-Mobile Ad hoc NETwork is kind of mobile multi hop wireless networks. Optimized Link State Routing Protocol is an optimization of classical Link State Routing Protocol, used for reducing network traffic. In LSR a node receiving a message or a packet must retransmit that message to all its neighbours who are one hop away from node. On the other hand OLSR uses concept of Multipoint Relays (MPRs) between their one hop neighbours in the network. OLSR works more efficiently in dense networks. OLSR uses HELLO and TC messages for communication. It's a Proactive routing protocol thus route is always available when any node want to transmit the packet. For this purpose HELLO messages are transmitted periodically for route discovery and TC messages are also generated when new mobile node is added to the network. In RFC of the OLSR, there is no security mechanisms are provided for security of the protocol. Flooding attack is a powerful attack which can take down the network with large number of unnecessary messages roaming around the network. Different solutions of some methods have been proposed for the same. In this paper we have studied these methods.

KEYWORDS: MANET, OLSR (Optimized link state routing), Flooding Disruption attack, Multipoint relays, Security, Flooding mechanisms

I. INTRODUCTION

A Mobile Ad hoc network is a multi hop routing network in which g group of mobile devices are capable of communicating wirelessly without using any centralized authority thus sending packets from one device to other via intermediates.

Different routing protocols exists for the packet transmission and communication in the network. Among which one protocol is OLSR Optimized Link State Routing Protocol.

OLSR uses a technique called Multipoint relays for transmission of messages among the nodes. MPR selection is used for the purpose. It is the process for the selection of the one hop neighbours to transmit the packets of any particular nodes further in the route. Each node will have its own MPR set through which it will transmit the control messages.

II. RELATED WORK

More work is done in MPR selection process to reduce the effects of flooding in the protocol OLSR.

The OLSR (Optimized Link State Routing) protocol is a proactive and table driven protocol designed for MANETs. It is a data gram protocol and it uses UDP port number 698. As it is a proactive protocol it provides the advantage of having routes immediately available whenever needed, not as reactive in which routes are discovered on demand.

In classical Link state routing, every received message is transmitted to its neighbour nodes while in OLSR the overhead is minimized through flooding of the control packets by using only subset of any particular node's neighbour nodes called Multipoint relays (MPRs). A set of MPR is a set of the nodes which are elected or chosen by the node to transmit its topology control messages to cover its all 2 hop neighbours in the network.

DOI: 10.15680/IJIRCCE.2015. 0311148

Two types of routing messages are periodically used by the OLSR for route discovery, which are 1. HELLO Message and 2. TC (Topology Control) message. HELLO packets are broadcasted to its neighbours after some constant time of interval. MPR is also select for all nodes as per the Willingness property of the nodes.

TC Message will be broadcasted in the whole network periodically by each MPR node to declare its MPR selector set, which is set of the nodes which have selected that particular node as its MPR, Meaning that set of the nodes for whom this particular node works as MPR.

Format of the both HELLO and TC message is shown in the following table.

One hop neighbor	Status of link	MPR set sq. no.	Mesg-sq.no.

(a) HELLO message

Originator Address	MPR selector-address	Message sq. no.	MPR selector set sq. no.	Hop count

(b) TC Message

Now, duplicate table is maintained by each node to identify duplicate TC message or to avoid reprocessing of same TC message by any node. Each node records recently received TC message until expiration of entry holding time in duplicate table. After information obtained from TC message, each node records topology information in topology table. This topology table also have information about MPR of other node in network. Now, routing table is constructed from the information of neighbour table and topology table. Routing table is updated if any of these tables (neighbour table and topology table) are changed. Entries for 1 hop neighbour as destination nodes are recorded in routing table from neighbour table and other entries are done by topology table. Routing table contains information of destination address, next hop and distance.

III. METHODOLOGIES USED

One technique to prevent flooding in OLSR is to mitigate the topology control traffic. New improved method of MPR selection is proposed to reduce the overheads generated by the redundant control information messages [1]. A function named k-robust-MPR is used to improve the selection of MPRs in network.

DOS is also used to flood the network and generate fake messages in the network. Mechanism called Denial Contradiction With Fictitious Node is proposed which checks some contradiction rules and offers fictitious node mechanism to prevent DOS (Denial of service attack) attack [2].

HOLSR is a protocol which was designed for the improved scalability of heterogeneous Mobile Ad hoc networks (MANETs), which is Hierarchical Optimized Link State Routing (HOLSR). Nodes are organized in cluster and Hierarchical topology control messages are used for inter cluster communication in the network [3].

In another method TC messages are transmitted using encryption and with the help of keys (public and private) and its secret share. Thus the integrity of the TC messages will not be compromised.

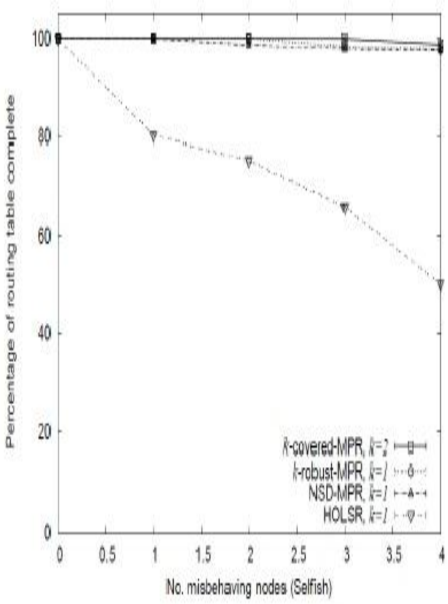
IV. EXPERIMENTS EVALUATION

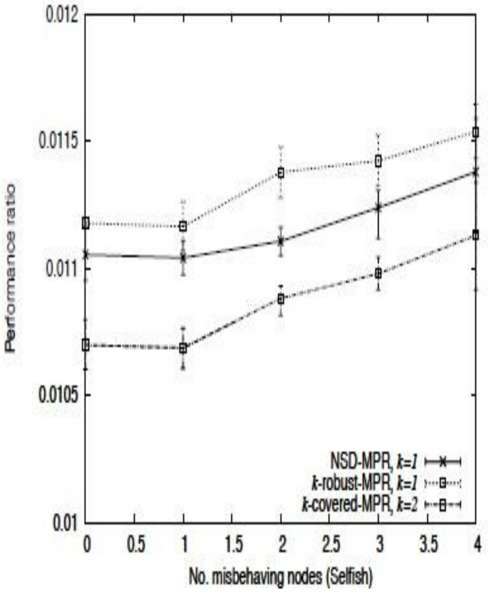
Simulations are conducted to assess the effectiveness of the proposed [3] countermeasures against flooding disruption attacks in HOLSR network. Number of the nodes are counted which are able to build complete routing tables under the presence of one to four attacker nodes.

Performance ratio is obtained as the percentage of nodes with complete routing tables over the number of the messages generated through the entire simulation. All experiments are conducted using the NS3 simulator [3].

Proposed countermeasures are tested in OLSR networks with three levels and 200 nodes in each case: one interface and 175 nodes and a transmission range of 100 m, two interface with 20 nodes and a transmission range of 200 m, three interface with five nodes and a transmission range of 500 m.

Following graph depicts the average number of nodes with complete routing tables and 95% of intervals of confidence which shows that how this strategies offer additional protection to mitigate the effect of the flooding and selfish nodes with selection of MPRs without a additional coverage using functions proposed for it. Thus K-robust MPR function mitigates the flooding.





(1) Percentage of node with routing table (complete)

(2)Performance ratio

V. CONCLUSION

Flooding is very powerful attack that can affect OLSR protocol. Some methods are proposed for the solution. These methods are studies in this paper and a survey is presented for the same. Other methods can be developed to detect and reduce or prevent flooding in OLSR as future work to control HELLO and TC messages in the network.

REFERENCES

[1] Gimer Cervera, Joaquin Garcia-Alfaro, Michel Barbeau and Evangelos Kranakis "Mitigation of Topology Control Traffic Attacks in OLSR Networks", School of Computer Science, Carleton University, Canada

[2] Nadav Schweitzer, Asaf Shabtai, Ariel Stulman Member of IEEE and Roy David Margalit "Mitigating Denial of Service Attacks in OLSR Protocol Using Fictitious Nodes", IEEE 2015

[3] Michel Barbeau, Gimer Cervera, Evangelos Kranakis and Joaquin Garcia-Alfaroy "Mitigation of Flooding Disruption Attacks in Hierarchical OLSR Networks", 2011 Ninth Annual Communication Networks and Services Research Conference, Schoo of Computer Science, Canada

[4] Chaitali Biswas Dutta, Utpal Biswas "Intrusion Detection System for Power-Aware OLSR", 2015 International Conference on Computational Intelligence & Networks, 2015 IEEE

BIOGRAPHY

Jigna B Bavaliya is a M.E. student at Atmiya institute of thechnology and science. She is doing masters in computer engineering.

Prof. Rashmi Agrawal is a Training & Placement officer at Atmiya instutue of technology and science, Rajkot, India

Prof. Archana Gondalaiya is an Assistant Professor at Atmiya instutue of technology and science, Rajkot, India