JCSE International Journal of Computer Sciences and Engineering Open Access

Research Paper Volume-6, Issue-4 E-ISSN: 2347-2693

Impact of Gray Holes on Optimized Link State Routing Protocol

G. Sumathi[1*], K.C. Aarthi[2], M. Shanmugapriya[3]

[1]Dept. of Computer Science and Engineering, Velammal Engineering College, Anna University, Chennai, India
[2] Dept. of Computer Science and Engineering, Velammal Engineering College, Anna University, Chennai, India
[3] Dept. of Computer Science and Engineering, Velammal Engineering College, Anna University, Chennai, India

**Corresponding Author: sumathi@velammal.edu.in, Tel.: 9361222594*

Available online at: www.ijcseonline.org

Received: 21/Mar/2018, Revised: 29/Mar/2018, Accepted: 20/Apr/2018, Published: 30/Apr/2018

Abstract— Mobile Ad hoc Network (MANET) is a set of wireless devices that can move around freely and cooperate with each other in relaying packets without the support of any fixed infrastructure or centralized administration. The absence of any central administration or base station in the MANET makes the routing between nodes more complex compared to wireless networks. Since MANETs are useful in disaster and military operations, the need for the group communication is vital. Most of the routing protocols proposed for ad hoc networks assume a trusted, non-adversial environment and do not take security issues into account in their design. But in real time a MANET is vulnerable to attacks than a wired or infrastructure wireless network. This thesis investigates the security of Optimized Link State Routing protocol (OLSR), a well known routing protocol in MANET by identifying the impact of malicious nodes called Gray Holes on it. Thus, a security extension to address the gray hole attack in OLSR routing has been proposed and the solution is achieved in a simulation environment using NS-2 simulator.

Keywords—MANET, infrastructureless network, OLSR, gray holes

I. Introduction

Ad hoc networks are a new paradigm of wireless communication for mobile hosts. Mobile Ad hoc Network (MANET) compromises of a set of wireless devices that can move around freely and cooperate with each other in relaying packets without the support of any fixed infrastructure or centralized administration. Hence they are known as infrastructure less networks. The mobile nodes operate with the help of battery power and they communicate with each other through antennas (transceiver – a transmitter and receiver) and the radio waves acts as the medium of communication.

The infrastructure less topology and dynamic reconfigurable nature of MANET makes it more difficult in finding the routes and providing security for data transmission. Here the routing and resource management are done in distributed manner in which all the nodes coordinate among them to enable communication. This requires each node to be more intelligent so that it can function both as a network host for transmitting and receiving data and network router routing packets from other nodes. Hence the mobile nodes in Ad hoc networks are more complex than their counterparts in wireless networks [1].

II. Objective

The main objective is to evaluate the impact of gray holes present in a MANET by detecting the gray holes and providing a countermeasure for the data packets that are selectively dropped by the gray holes, using OLSR as the routing protocol.

III. Optimized Link State Routing Protocol (OLSR)

The Optimized Link State Routing protocol (OLSR) is a proactive link state routing protocol. Due to its proactive nature, it has an advantage of having the routes immediately available when needed. In pure link state protocol, all the links with neighbor nodes are declared and are flooded in the entire network. OLSR protocol is an optimization of a pure link state protocol for MANETS [2].

In OLSR routing protocol, there are two types of control packets used: *Hello* packets and *Topology Control* packets (TC). Hello packets are used to build the neighborhood of a node and to discover the nodes that are within the environs of the node. And this also used to compute the multi-hop relays of a node. The OLSR protocol uses the periodic broadcast of hello packets to establish the connection [3].

The Hello messages are received by all one-hop neighbors, but the Hello messages are not forwarded to other nodes by the received node. This hello message broadcasting will happen for every fixed interval; this is known as Hello interval. This allows the nodes to discover its two-hop neighbors since the node can passively listen to the transmission of its one-hop neighbor. The status of these links with the other nodes in its neighborhood can be asymmetric, symmetric or Multi Point Relay (MPR).

The main advantage of using OLSR is it does not require that the link reliable for the control messages. The messages will be sent periodically and the delivery does not have to be sequential. The OLSR is easy to integrate with existing operating systems and it only interacts with the host routing table. This is more suitable for the application, which needs fast data transmission of the data packets with low delay [3]. The main process of OLSR is as follows.

- Neighbor sensing
- MPR (Multi Point Relay) selection
- MPR information declaration
- Route table calculation.

The main drawback of OLSR is it needs more time to rediscover a broken link. And it also needs more processing power at the time alternate route discovery. With the security constraint, in OLSR all the control messages are needed to be secured and also the host and gateways should be statically configured in order to advertise the routes to the valid addresses [3].

IV. Gray Holes

Gray holes are malicious nodes present in the network. These nodes are a refined version of black holes. In black hole attack the malicious node discards all the packets completely and does not forward any packet [4]. Whereas, in gray hole attack, the malicious node discards only selected packets and forwards other packets. This makes the detection of malicious node difficult. Since these nodes do not drop all packets and forward selective packets, this attack is also known as selective forwarding attack [5].

V. Detection of Gray Holes

In order to demonstrate the impact of gray hole nodes, their presence is detected using Two Hop Acknowledgement (THA) method [1]. The working of THA is given below.

- First, node A send packet to node C through node B.
- Then node A request hop-table from node C to verify recently sent packet was updated or not.
- To detect the gray hole node, the reply for the above request doesn't come within the TTL (or) Time stamp then the node B can identified as a gray hole node.

A. Algorithm for Two Hop Acknowledgement

Notations:
SN: Source Node
IN: Intermediate Node
DN: Destination Node
NHN: Next hop Node
THA: Two hop acknowledgement
FRq: Further Request
FRp: Further Replay
DRI: Data routing information
ID: Identity of the node

```
SN broadcast RREQ
SN receiver RREP
if (RREP is from DN or a Reliable Node){
    Route data packet (Secure Route)
else {
    Send FRQ and ID of IN to NHN
    Receive FRp, NHN of current NHN, DRI
    entry
    for NHN's next hop, DRI entry for current IN
    If (NHN is a reliable Node)
        Check IN for gray hole Node using THA
        if (IN is not a gray hole Node)
            data packet(secure Route)
        else {
            insecure rote
            IN is a gray hole node
            do
            Secure message transmission ( )
            do
            current IN =NHN
        }
}
```

B. Algorithm Description

If the source node broadcasts the RREQs Packet,it is passed on all the routes from that source node and after the destination node receiving the RREQs then forward the RREPs using the reverse route .if the RREPs comes from the reliable intermediate node then send the data packets else ask for further Request and if the node is detected to be a gray hole node by the two hop acknowledgement method (i.e.if the data routing information is not updated) then to provide solution to the attack perform secure massage transmission. In Case of Secure message transmission, the data packets are transmitted with the redundancy bits and if the node behaves gray hole then the original packets can be relayed depending on the redundancy ratio(n out of m packets).if the node is not the gray hole node then forward the packets directly. When the node gets attacked the packet delivery gets decreased and control overhead increases.

VI. Countermeasure for Gray Hole Attack

The data packets that have been selectively dropped by the gray hole nodes are recovered successfully at the receiver side by using redundancy bit mechanism. In this mechanism, first the message along with the redundancy bit is sent to the receiver, where the redundancy bit are divided into number of pieces , so that even a partial reception can lead to the successful reconstruction of the message at the receiver. In principle, the encoding (and dispersion) allows the reconstruction of the original message with successful reception of any M out of N transmitted pieces (Figure 1). The ratio **r=N/M** is termed as redundancy factor.

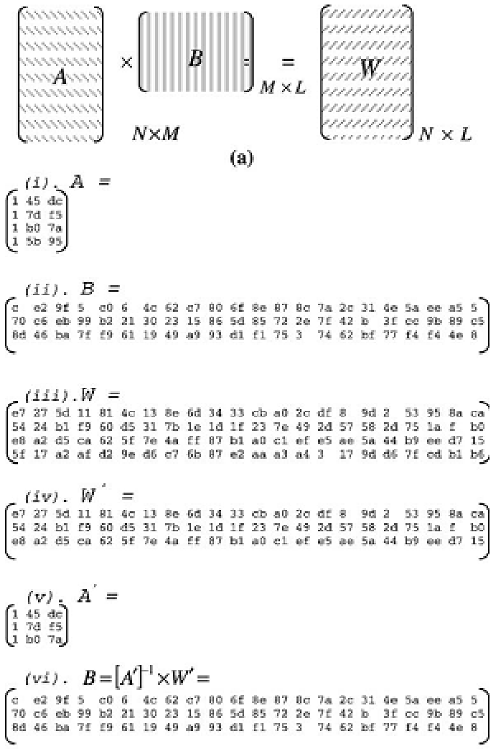

Figure 1. Redundancy Bit Mechanism

VII. Simulation and Results

The detection of gray holes and the solution to recover the data loss caused by these nodes are implemented using NS-2 simulator, a scalable simulation environment for large scale wireless communication networks. In this simulation, networks with 50 mobile nodes are taken. In order to evaluate the performance of the proposed solution, three different scenarios namely, network with gray hole attack, network without attack and network with solution for gray hole attack are taken under consideration. All the three scenarios namely are placed in 1000X1000 terrain. Each source transmits a maximum of 100 packets (512 bytes each) at various times during the simulation.

To evaluate the performance of the network at various scenarios, the following metrics are used.

A. Packet Delivery Ratio

Packet delivery ratio is defined as the data packets delivered divided by the data packets expected to be delivered [1].

B. Control Overhead

Control overhead is defined as control packets transmitted divided by the data packets delivered [1].

C. Total Overhead

Total overhead is defined as packets transmitted (control packets +data packets) divided by the data packets delivered [1].

Simulation Parameters are shown in the following table.

Table 1. Simulation Parameters

PARAMETER	VALUE	DESCRIPTION
NO. OF MOBILE NODES	50	Simulation node
TYPE OF CHANNEL	Wireless	Channel type
TYPE OF PROPAGATION	Two Ray Ground	Radio-propagation model
TYPE OF NETWORK INTERFACE	Phy/WirelessPhy	Network interface type
TYPE OF INTERFACE QUEUE	Queue/DropTail/Pri Queue	Interface queue
TYPE OF ANTENNA	Antenna/OmniAnte nna	Antenna model
TYPE OF PROTOCOL	OLSR	Optimized Link State Routing protocol
SIMULATION TIME	50m	Maximum simulation time
PACKET SIZE	512bytes	Data packet size
TERRAIN DIMENSIONS	1000m 1000m	x- dimension of motion y- dimension of motion

VIII. Performance Evaluation of Gray Hole Attack

A. Packet Delivery Ratio

Figure 2 shows the comparison between Packet delivery ratio and number of nodes for three scenarios namely without attack, with attack and with solution. From the figure, it is clear that packet delivery ratio decreases when there is attack but increases when the solution is provided to the range of packet delivery ratio without attack.

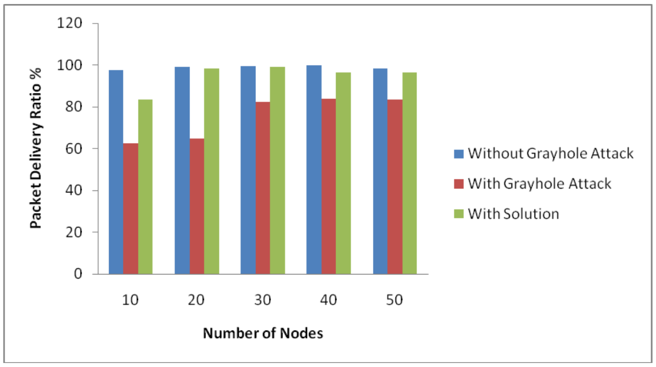

Figure 2. Packet Delivery Ratio for Gray hole Attack

B. *Control Overhead*

Figure 3 shows the comparison between Control Overhead and number of nodes for three scenarios namely without attack, with attack and with solution. From the figure, it is clear that Control Overhead increases when there is attack but decreases when the solution is provided to the range of control overhead without attack.

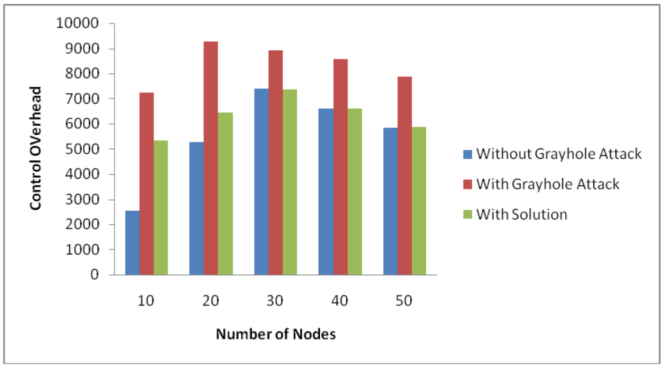

Figure 3. Control Overhead for Gray hole Attack

C. *Total Overhead*

Figure 4 shows the comparison between total Overhead and number of multicast group for three scenarios namely without attack, with attack and with solution. From the figure, it is clear that total overhead increases when there is attack but decreases when the solution is provided to the range of Total Overhead ratio without attack.

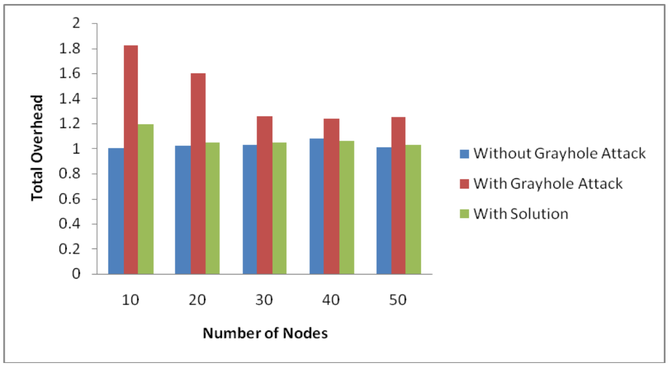

Figure 4. Total Overhead for Gray hole Attack

IX. CONCLUSION

The performance of a Mobile Ad hoc Networks under attack depends heavily on many factors such as the number of senders, the number of receivers, the number of attackers as well as their positions. Here thorough description of OSLR protocol and how the protocol can be made more secure by providing a solution on the gray hole attack is provided. The various scenarios during which a node may selectively drop packets are analyzed.

X. REFERENCES

[1] P. Sankareswary, R. Suganthi, G. Sumathi "*Impact of Gray hole nodes in Multicast Adhoc On Demand Distance Vector Protocol* ", In the Proceedings of the 2010 IEEE International Conference ICWCSC 2010, SSN Engineering College, Chennai, India, 2010

[2] P. Jacquet, P. Muhlethaler, T. Clausen, A. Laouiti, A. Qayyum, L. Viennot, "*Optimized Link State Routing Protocol for Ad Hoc Networks*", Hipercom Project, INRIA Rocquencourt, BP 105, 78153 Le Chesnay Cedex, France.

[3] L. M. Mary Jelba, S. Gomathi, "*Mitigating Different Attacks in OLSR Protocol – A Survey*", International Journal of Inovative Research in Computer Science and Communication Engineering, Vol.4, Issue 6, June 2016

[4] S. Sharma and R. Gupta, "*Simulation Study of black hole attack in the mobile ad hoc networks*", Journal of Engineering Science and Technology, pp.243-250, 2009.

[5] Kshitij Bhargava, Dinesh Goyal, "*Packet Dropping Attacks in Manet: A Survey*", Journal of Advanced Computing and Communication Technologies, Vol.2, Issue No.3, June 2014

[6] Rupali Sharma, "*Gray-hole Aattack in Mobile Ad-hoc Networks: A Survey*", International Journal of Computer Science and Information Technologies, Vol.7, Issue.3, 2016

[7] Biswaraj Sen, Kalpana Sharma, M.K.Ghose, Achute Sharma "*Gray Hole Attack in MANETs*", International Journal of Advances in Electronics and Computer Science, Vol.2, Issue.10, Oct, 2015.

[8] Onkar V. Chandure, V.T.Gaikwad, "*Detection & Prevention of Gray Hole Attack in Mobile Ad-Hoc Network using AODV Routing Protocol,*" International Journal of Computer Applications , Vol.41, Issue.5, March, 2012

[9] S.V. Vasantha, Dr.A. Damodaram, *"A Defense Model for Black hole and Gray hole Attacks in MANET*", IJCSMC, Vol.3, Issue. 11 pp.570-576, 2014.

[10] Madhuri Gupta, Krishna Kumar Joshi, "*A Review on Detection and Prevention of Gray-Hole Attack in MANETs*", International Journal of Scientific & Engineering Research, Vol.4, Issue.11, November, 2013.

Authors Profile

Mrs. G. Sumathi pursed Bachelor of Technology in Computer Science and Engineering from Rajiv Gandhi College of Engineering and Technology, affiliated to Pondicherry University in the year 2010 and Master of Technology in Computer Science and Engineering from Sri Manakula Vinayagar Engineering College affiliated to Pondicherry University in the year 2012. She is currently working as Assistant Professor in Department of Computer Science and Engineering, Velammal Engineering College, affiliated to Anna University, Chennai, Tamil Nadu, India. She has published more than 10 research papers in reputed international journals and conferences and it's also available online. Her main research work focuses on Network Security, Artificial Intelligence, Machine Learning and Cloud Computing. She has 4 years of experience in teaching.

Mrs. K. C. Aarthi pursed Bachelor of Technology in Computer Science and Engineering from Avinashilingam University, Faculty of Engineering, Coimbatore in the year 2011, and Master of Technology in Information Technology from Velammal Engineering College affiliated to Anna University in the year 2013. She is currently working as Assistant Professor in Department of Computer Science and Engineering, Velammal Engineering College, affiliated to Anna University, Chennai, Tamil Nadu, India. Her main research work focuses on Network Security and Cloud Computing. She has 3 years of experience in teaching.

Mrs. M. Shanmughapriya pursed Bachelor of Technology in Computer Science and Engineering from KLN College of Information and Technology, affiliated to Anna University in the year 2007 and Master of Technology in Computer Science and Engineering from Velammal Engineering College affiliated to Anna University in the year 2017. She is currently working as Assistant Professor in Department of Computer Science and Engineering, Velammal Engineering College, affiliated to Anna University, Chennai, Tamil Nadu, India. She has published more than 4 research papers in reputed international journals and conferences and it's also available online. Her main research work focuses on Artificial Intelligence, Machine Learning and Cloud Comuting. She has 1 years of experience in teaching and 4.2 years of industrial experience in software development and maintenance.