Volume 1, Issue 4, October 2014 ISSN: 2348-8565 (Online)

International Journal of Modern Engineering and Research Technology

Website: http://www.ijmert.org Email: editor.ijmert@gmail.com

Simulation of Grayhole Attack

Dr. Mamta Lambert
Associate Professor
Department of Computer Applications
Jabalpur Engineering College Jabalpur,
Jabalpur (M.P.) [INDIA]
Email: lambert_mamta@yahoo.co.in

Sharda Prasad Patel
Email: sharda21patel@gmail.com

ABSTRACT

Mobile ad hoc network (MANET) is a self-configuring network of mobile nodes formed anytime and anywhere without the help of a fixed infrastructure or centralized management. Due to open, dynamic, infrastructure-less nature, the ad hoc networks are vulnerable to various attacks. AODV is an important on-demand distance vector routing protocol for mobile ad-hoc networks. We are using AODV protocol for simulation with a gray hole node which drops the packet. To improve the performance we are using IDSaodv technique, which enable us to minimize the attacks.

Keywords:—*MANET, AODV, Routing Protocols, grayhole node, malicious node.*

I. INTRODUCTION

In an ad-hoc network, mobile nodes communicate with each other using multihop wireless links. The infrastructure is not fixed that is changing with dynamic topology. Each node in the network acts as a router, forwarding data packets to other nodes.

MANET have many potential applications, in military rescue operations and commercial environments. Mobile ad hoc networks are having several security issues due to their inherent nature, like open medium, dynamic topology, lack of centralized control, limited battery power and limited bandwidth. Hence, there exist several attacks that can be easily launched on an ad hoc network. Since, wireless networks came into existence, routing in mobile ad hoc networks has been a challenging task. The major reason for this is the constant changes in network topology due to the mobility of nodes.[14]

Mobile Adhoc Network

Figure 1. MANET

II. SECURITY ATTACK

In recent times we have seen a variety of attacks have been identified and detected in the network[17]. To provide a secure communication in the network we need to face the security challenges [6]. There are two major categories where we have to consider always in the security attacks, they are

Passive attacks:

A passive attack won’t interrupt the normal operation of MANET, while data have been exchanged from the network. The solely nature of passive attack is to identify the data exchanged in the network. The attacker snoops the data exchanged in the network without altering it. Here the requirements of confidentially gets violated.

B. Active attacks:

An Active attack always tries to modify the normal operation of MANET, which means the interruption have been made in the network, such as doing data interruption, modification, deletion and fabrication. Active attacks can be internal or external.

Table 1: Security Attacks Classification

Passive Attacks	Eavesdropping, traffic analysis, monitoring
Active Attacks	Jamming, spoofing, modification, replaying, DoS

Protocols Used In MANET

In MANET nodes communicate with each other by using some routing protocols. According the dynamic topology and characteristic there are three main routing protocol used in MANETs. These all are discussed below.

Reactive (On-Demand) Routing Protocol:

This protocol starts functioning whenever any node wants to transmit data to other node. In this protocol network bandwidth is not wasted and network is less congested. This protocol is less secure than the proactive protocols. Two kinds of protocols are there in it Adhoc On Demand Distance Vector (AODV) protocol, Dynamic Source Routing (DSR) protocol.

Proactive (Table Driven) Routing Protocol:

This protocol is also called as table driven protocol because in this protocol each node in the network maintains its detailed routing table. These all are discussed below.

In the routing table each node maintain complete path to the reachable node with its hop count. In this, each node periodically broadcast their routing information to the neighbors. Periodically update and large routing table generate large amount of overhead in the network which makes this protocol unusable. There are two main kind of this protocol optimized link state routing

(OLSR) protocol and destination sequenced distance vector routing (DSDV) protocol.

Hybrid Routing Protocol:

This protocol combines advantages of both proactive and reactive routing protocol. Two types are: Zone routing protocol (ZRP) and temporally ordered Routing protocol (TORA). At the initialization phase this follows proactive characteristic after that in between when network topology has changed it follows reactive characteristic.

Overview of AODV Routing Protocol :

The Ad hoc On-demand Distance Vector (AODV) is a widely used simple, efficient and effective routing protocol. It typically minimizes the number of required broadcasts by creating routes on a demand basis, when a source node wishes to route a packet to a destination node, it uses the specified route if afresh enough route to the destination node is available in its routing table. If not, it starts with a route discovery process by broadcasting the Route Request (RREQ) message to its neighbors, which is further propagated while it reaches an intermediate node with afresh enough route to the destination node specified in the RREQ, or the destination node itself. AODV make a route using a route request / route reply query cycle. [16]

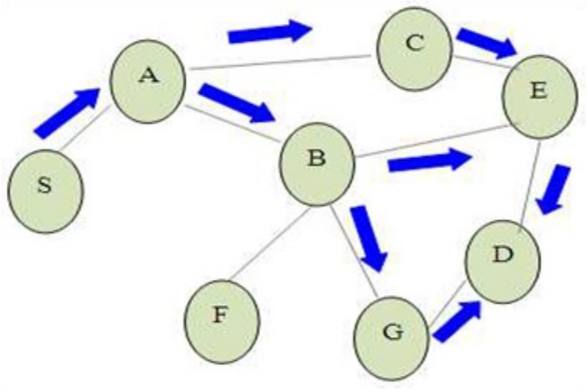

Figure 2. AODV route discovery using RREQ Packet

III. Gray Hole Attack

This kind of dropping against black hole, does not drop all data packets. Attacker drops occasionally packets. It means attacker sometimes acts like a normal node and other times as a malicious node.[1]

The Gray Hole attack has two phases. Initially, a malicious node exploits the AODV protocol to advertise itself as having a valid route to a destination node, with the intention of intercepting packets, even though the route is spurious. Next, the node drops the intercepted packets with a certain probability. This attack is more difficult to detect than the black Hole attack where the malicious node drops the received data packets with certainty. A Gray Hole may exhibit its malicious behavior in various techniques. It simply drops packets coming from (or destined to) certain specific node(s) in the network while forwarding all the packets for other nodes. Another type of Gray Hole attack is a node behaves maliciously for some particular time duration by dropping packets but may switch to normal behavior later. A Gray Hole may also exhibit a behavior which is a combination of the above two, thereby making its detection even more difficult.[3]

1-source node
8-destination node

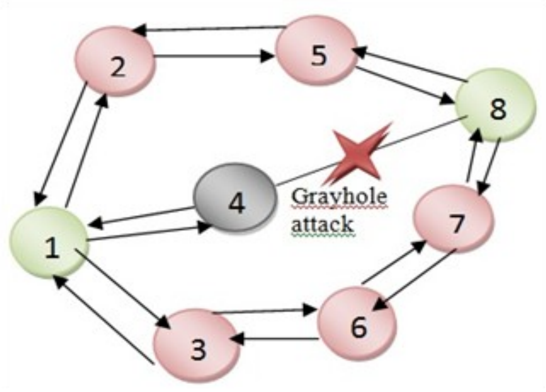

Figure 3. Grayhole Attack

IV. Literature Review

1. S Banerjee et.al.[6] have proposed the algorithm to prevent Black/Gray hole attacks.

In this paper we have studied the work that attempt to detect black or gray hole or cooperative black and gray hole attack. Finally they proposed a feasible solution for detection and removal of chain of cooperative black and gray hole attack in AODV protocol. In solution each node can locally maintain its own table of black listed nodes whenever it tries to send data to any destination node and it can also aware the network about the black listed nodes. This list of malicious nodes can be applied to discover secure paths from source to destination by avoiding multiple black/ gray hole nodes acting in cooperation.[6]

2. Mr. Chetan S.Dhamandel1, Prof. H.R.Deshmukh2 1ME Scholar, CSE (First Year), B.N.C.O.E, Pusad (MS) INDIA 2 Associate Professor, Dept of CSE, B.N.C.O.E, Pusad (MS) INDIA.

In this paper, first set the waiting time for the source node to receive the RREQ coming from other nodes and then add the current time with the waiting time. Then in storing process, store all the RREQ Destination Sequence Number (DSN) and its Node ID n RR-Table until the computed time exceeds. Generally the first route reply will be from the malicious node with high destination sequence number, which is stored as the first entry in the RR-Table. Then compare the first destination sequence number with the source node sequence number, if there exists much more differences between them, surely that node is the malicious node, immediately remove that entry from the RR-Table. This is how malicious node is recognized and eradicate. Final process is selecting the next node id that has the higher destination sequence number, is obtained by sorting the RR-Table according to the DSEQ-NO column, whose packet is sent to malicious node recognition in order to continue the default operations of AODV protocol.[15]

3. Maha Abdelhaq et. al "A Local Intrusion Detection Routing Security over MANET Network" 2011 International Conference on Electrical Engineering and Informatics, 2011 IEEE.

In these authors proposed Local Intrusion Detection (LID) security mechanism. This mechanism allows the detection of malicious node by using Further Route Request (FRREQ) and Further Route Reply (FRREP) packet. When any intermediate node (say n) to source node received RREP packet, it performs LID. An intermediate node buffers the RREP packet and send FRREQ packet to next node using new route. The next node replies by using FRREP packet. This intermediate node extracts information and behaves accordingly.[12]

4. Kurosawa, S., Nakayama, H., Kato, N., Jamalipour, A., and Nemoto, Y. 2007.

Another algorithm is considering a limit for sequence number. When source node receives RREP packets, it checks them with a threshold for sequence number of that route and if the received RREP sequence number is higher than that, source enters that node ID in a blocked list and announces that node as malicious to all nodes by broadcasting its ID; because in Gray hole, attacker starts dropping packets by announcing itself as a node has the freshest route to destination. This sequence number threshold is calculated by average of table's entries sequence numbers in a certain period of time. [13]

Advantages

Main benefit of this method is simplicity.

On the contrary of other methods, no energy is consumed for monitoring.

Disadvantages

This algorithm does not detect any grayhole attacks. This method may also make mistake when a node is not malicious, but according to its higher sequence number may be entered into blocked list.

5. Vishnu K B.tech V sem MNNIT Allahabad INDIA. 2010 International Journal of Computer Applications (0975 - 8887) Volume 1 – No. 22.

The main idea behind this method is to list out the set of malicious nodes locally at each node whenever they act as a source node. As mentioned in the Assumption our protocol uses the concept of Core Maintenance of the Allocation Table i.e., whenever a new node joins the network, it sends a broadcast message as a request for IP address. The backbone node on receiving this message randomly selects one of the free IP addresses. The new node on receiving the allotted IP address sends an acknowledgement to the BBN. Now since the allocation is only under the control of the Back Bone Nodes (BBN) the dynamic pool of unused/restricted IPs of the network at any point of time is known only to the BBN.[9]

V. IMPLEMENTATION

An IDS is a second protection for MANETs security. An intrusion detection system is system software used to analyze malicious behaviors network and generate reports. It can be defined as a process of monitoring the events occurs in the computer system or network and analyzing for an intrusions dealing with confidentiality, integrity and availability of a computer system.

For implementing gray hole we have done changes in tcl file in ns2. We have addad grayholeaodv in ns-lib.tcl.then we also add grayholeaodv in make file present in ns-2.34 folder.this line is added in ns-lib.tcl.

```
grayholeAODV
{set ragent [$self create-grayholeaodv-
agent $node]}
```

For creating grayholeaodv agent add the following code in ns-lib.tcl.

```
Simulator instproc create-grayholeaodv-
agent
{ node }
{ # Create grayholeAODV routing agent
set ragent
[new Agent/grayholeAODV [$node node-
addr]]
$self at 0.0 "$ragent start" ;
# start BEACON/HELLO Messages
 $node set ragent_ $ragent
```

Add graholeaodv protocol in make file by adding code given below.

```
grayholeaodv/grayholeaodv_logs.o gray-
holeaodv/grayholeaodv.o\ grayholeaodv/
grayholeaodv_rtable.o grayholeaodv/
```

Similarly for adding IDSaodv protocol the same changes have to be done as we did for grayholeaodv protocol.e have to add idsaodv protocol in ns-lib.tcl and make file.

VI. Simulation

We use NS-2 (v-2.34), a network simulation tool to simulate wireless and wired communication network. NS2 is discrete event simulator developed by the University of California in Berkeley. It provides a good platform for MANET simulation. We simulate our model for 15, 25 and 35 nodes.

Table 2. The simulation parameters

Parameter	Definition
Protocol	aodv, grayholeaodv, idsaodv
MAC layer	IEEE 802.11
Simulation duration	100s
Node placement	Random
Simulation area	500m x 500m
Traffic sources	CBR
Number of nodes	15, 25,35
Pause time	5s
Version NS-2	2.34

Performance Metrics

Some important performance metrics can be evaluated:-

Packet delivery fraction — The ratio of the data packets delivered to the destinations to those generated by the CBR sources.

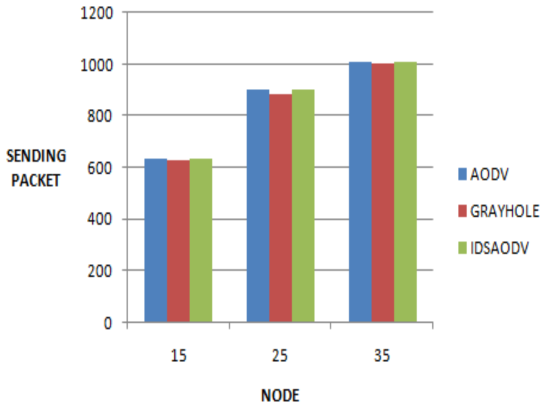

Figure 4: Sending packets values for different nodes.

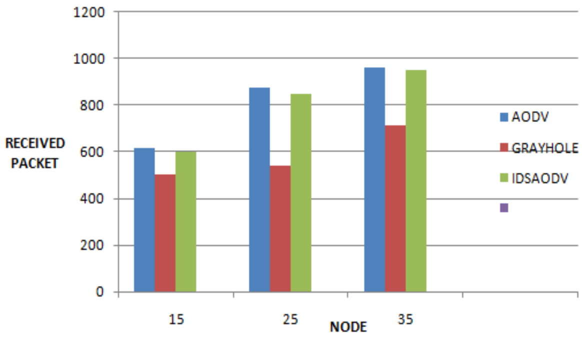

Figure 5: Received packets values for different nodes.

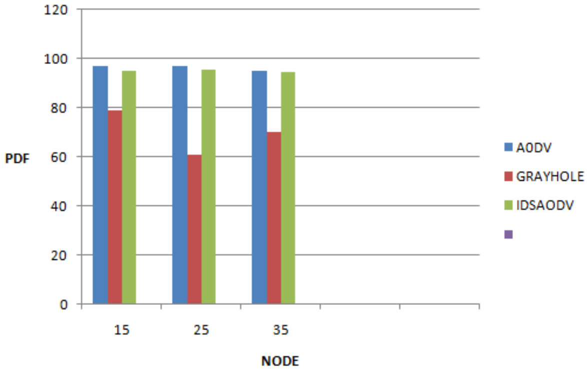

Figure 6: PDF values for different nodes.

VII. Conclusion

Detection of gray hole is more difficult than black hole, because the attacker works as normal node then starts dropping of data. In this paper, we introduced some of the comparison between readings of aodv, grayhole, and idsaodv. And we can see that when grayhole node is introduced, performance decreases, and after applying IDS technique performance get improved.

VIII. Future Work

In this paper we have measured the effect of gray hole attack and try to improve performance by using IDS technique by comparing different parameters. The same scenario can also be applied for different protocol like DSR, etc.

REFERENCES:

[1] “Methods of Preventing and Detecting Black/Gray Hole Attacks on AODV-based MANET” Marjan Kuchaki Rafsanjani Department of Computer Science, Shahid Bahonar University of Kerman, Kerman, Iran IJCA Special Issue on “Network Security and Cryptography” NSC, 2011.

[2] “Grayhole Attack and Prevention in Mobile Adhoc Network” Megha Arya SATI (vidisha) SATI Sagar Road Vidisha M.P, India. International Journal of Computer Applications (0975 – 8887) Volume 27– No.10, August 2011.

[3] “Comparing the impact of Black Hole and Gray Hole Attacks in Mobile Adhoc Networks”, Usha and Bose Department of Computer Science and Engineering, Faculty of Information and Communication Engineering, Anna University, Chennai, 600 025, India Journal of Computer Science 2012, 8 (11), 1788-1802

[4] “An Effective Intrusion Detection System for Detection and Correction of Gray Hole Attack in MANETs”, Shivani Sharma Assistant Professor, Tanu Preet Singh Assistant Professor International Journal of Computer Applications (0975 – 8887) Volume 68– No.12, April 2013.

[5] “A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks”, Bing Wu, Jianmin Chen, Jie Wu, Mihaela Cardei Department of Computer Science and Engineering Florida Atlantic University WIRELESS/MOBILE NETWORK SECURITY Y. Xiao, X. Shen, and D. -Z. Du (Eds.) 2006 Springer.

[6] “Detection/Removal of Cooperative Black and Gray Hole Attack in

Mobile Ad- Hoc Networks", Sukla Banerjee, Proceedings of the World Congress on Engineering and Computer Science 2008 WCECS 2008, October 22 - 24, 2008, San Francisco, USA.

[7] "A Literature Survey of Black Hole Attack on AODV Routing Protocol" Chandni Garg1, Preeti Sharma2, Prashant Rewagad3 International Journal of advancement in electronics and computer engineering (IJAECE) Volume 1, Issue 6, Sep 2012.

[8] "Advanced Algorithm for Detection and Prevention of Cooperative Black and Gray Hole Attacks in Mobile Ad Hoc Networks", Shalini Jain, ©2010 International Journal of Computer Applications (0975 – 8887) Volume 1 – No. 7.

[9] "Detection and Removal of Cooperative Black/Gray hole attack in Mobile ADHOC Networks", Amos J Paul, ©2010 International Journal of Computer Applications (0975 - 8887) Volume 1 – No. 22.

[10] "Detection & Prevention of Gray Hole Attack in Mobile Ad-Hoc Network using AODV Routing Protocol" Onkar V.Chandure International Journal of Computer Applications (0975 – 8887) Volume 41– No.5, March 2012.

[11] "Multiple Black Hole Node Attack Detection Scheme in MANET by Modifying AODV Protocol" Nishu kalia, Kundan Munjal, International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-2, Issue-3, February 2013.

[12] Maha Abdelhaq et. al "A Local Intrusion Detection Routing Security over MANET Network" 2011 International Conference on Electrical Engineering and Informatics, 2011 IEEE.

[13] Kurosawa, S., Nakayama, H., Kato, N., Jamalipour, A., and Nemoto, Y. 2007. "Detecting black hole attack on aodv-based mobile adhoc networks by dynamic learning method". J. Network Security. Vol. 5, No. 3 (Nov. 2007), 338–346.

[14] "Detection & Prevention Techniques to Black & Gray Hole Attacks In MANET: A Survey" Nitesh A. Funde1, P. R. Pardhi2 M Tech Scholar, Department of Computer Science, RCOEM, Nagpur, India 1 Professor, Department of Computer Science, RCOEM, Nagpur, India.

[15] "A Efficient Way To Minimize the Impact of Gray Hole Attack in Adhoc Network" Mr.Chetan S.Dhamande1, Prof H.R.Deshmukh2 1ME Scholar, CSE (First Year), B.N.C.O.E, Pusad (MS) INDIA 2Associate Professor, Dept of CSE, B.N.C.O.E,Pusad (MS) INDIA.

[16] "A Survey on Detection and Prevention Techniques for Gray-Hole Attack in MANET", Mahesh Kumar Kumawat, Jitendra Singh Yadav.

[17] "A Survey on Gray Hole Attack in MANET", V. SHANMUGANATHAN, Master of Computer Science and Engineering, K.S.R. College of Engineering, Tiruchengode, India.

* * * * *