Simulation of Gray Hole Attack in Adhoc Network Using NS2

Ms. Meenakshi
Research Scholar, M.Tech (CSE)
Department of Computer Science and Applications
Chaudhary Devi Lal University
Sirsa, Haryana, India
meenakshi_hsr@rediffmail.com

Mr. Kapil Kumar Kaswan
Department of Computer Science and Applications
Chaudhary Devi Lal University
Sirsa, Haryana, India
kapilkaswan@gmail.com

Abstract—A Wireless ad-hoc network is a short-lived network set up by wireless mobile computers or nodes moving randomly in the places that have no network infrastructure. While the nodes communicate with each other, they assist by forwarding data packets to other nodes in the network. Thus the nodes discover a path to the destination node using routing protocols. Though, due to safety measures of the routing protocols, wireless ad-hoc networks are undefended to attacks of the malicious nodes. One of these attacks is the Gray Hole Attack against network integrity absorb all data packets in the network and data packets do not connect with the destination node. As a result data loss will occur. There are many detection and protection procedures to reduce the intruder that perform the gray hole attack. In this paper, simulate the gray hole attack in AODV This paper analyze the effect of gray hole attack on MANET and detection of these attacks by using IDS.

Keywords: MANET, Gray Hole, Intrusion Detection System (IDS)

I. INTRODUCTION

A Wireless networks assign quick access to information and computing, reducing the barriers of distance, time, and location for lots of application ranging from mutual, distributed mobile computing to disaster recovery. Ad hoc Network means a network without any base stations “infrastructure-less” or multi-hop. It is collection of devices equipped with wireless communications and networking capability. A Wireless Ad Hoc Network is a decentralized wireless network. The network is ad hoc because each node is willing to forward data for other nodes, and so the determination of which nodes forward data is made dynamically based on the network connectivity. This is in contrast to wired networks in which routers perform the task of routing. The decentralized nature of wireless ad hoc networks makes them suitable for a variety of applications where central nodes can't be relied on, and may improve the scalability of wireless ad hoc networks compared to wireless managed networks, though theoretical and practical limits to the overall capacity of such networks have been identified.

Minimal configuration and quick deployment make ad hoc networks suitable for emergency situations like natural disasters or military conflicts. The presence of a dynamic and adaptive routing protocol will enable ad hoc networks to be formed quickly. routing protocols for wired networks cannot be directly used in wireless networks and numerous protocols have been developed for Ad Hoc Networks. These routing protocols are divided into two categories based on management of routing tables. These categories are Table Driven Routing Protocols and On-Demand Routing Protocols, shown in the Table 1.

Routing protocols are divided into two categories. These categories are Table Driven Routing Protocols and On-Demand Routing Protocols. In Table Driven Routing Protocols, each node maintain reliable routing tables, every node propagates the update messages to the network when the network topology changes. It periodically updating the network topology increases bandwidth overhead, and periodically updating route tables keeps the nodes awake and abruptly consume their batteries, many unnecessary route entries to the specific destination take place in the routing tables. In On-Demand Routing protocols route tables are created when required. When the source node requires connecting to the destination node, it broadcast the route request packet to its neighbors. The route remains in the route tables of the nodes through shortest path until the route is no longer needed.

Table Driven Routing Protocols	On-Demand Routing Protocols
Destination-Sequenced Distance Vector Routing Protocol (DSDV)	Cluster based Routing Protocols (CBRP)
Fisheye State Routing (FSR)	Ad-Hoc On-Demand Distance Vector Routing (AODV)
Wireless Routing Protocol (WRP)	Signal Stability Routing (SSR)
Global State Routing (GSR)	Dynamic Source Routing Protocol (DSRP)
Hierarchical State Routing (HSR)	Associativity Based Routing (ABR),
Zone-based Hierarchical Link State Routing Protocol(ZHLS)	Temporally Ordered Routing Algorithm (TORA)
Clusterhead Gateway Switch Routing Protocol (CGSR)	

Table 1 – Ad Hoc Networks routing protocols

II. AD-HOC ON-DEMAND DISTANCE VECTOR (AODV)

In this paper, AODV used for implementation of Gray Hole attack with this protocol. Ad–hoc on demand distance vector routing (AODV) is on-demand routing protocol. It is classified under reactive protocol. Functions of AODV protocol is route discovery and route maintenance. In Ad-hoc routing, when a route is required particular destination, the protocol establish route discovery. Route discovery process begins with the creation of a Route Request (RREQ) packet. The packet contains source node's IP address, source node's current sequence number, destination IP address, destination sequence number the broadcast identifier and the time to live field. AODV uses a destination sequence number to determine up-to-date path to the destination. A node updates its path information only if the sequence number of the current packet received is greater or equal than the last sequence number stored at the node. Destination sequence number indicates the freshness of the route that is accepted by the source. All intermediate nodes having valid routes to the destination, or the destination node itself, are allowed to send Route Reply packets to the source. Every intermediate node, while forwarding a Route Request, enters the previous node address and it's Broadcast id. When a node receives a Route Reply packet, information about the previous node from which the packet was received is also stored in order to forward the data packet to this next node as the next hop toward the destination.

Ad hoc networks attacks risk not only from outside but also from inside. These attacks can be active as well as passive. Passive attacks involve only eavesdropping on the data that is communicated in the network. In Active attacks attacker attempts to alter or change data that is being exchange in the network. Attacks also be classified as Internal and External attack. External attack carried out by the node that does not belong to the domain of the network and internal attacks are from compromised nodes which are actually part of network. There are two main methods to secure the network. Intrusion Prevention and Intrusion Detection approach. Intrusion Prevention method is able to handle external attacks as we can assume that the intruders don't have access to the network cryptosystem e.g. they don't have confidential key specifically accepted in the network. So, digital signatures scheme can be used to defend information validity and reliability. Whereas the intrusion prevention method be able to reduce interruptions, none are fully enough to protect ad hoc networks. Inadequacies of Intrusion Prevention enhance the overhead throughout usual process of Ad Hoc networks. So there is need of second wall of defense in ad hoc networks. Second approach is Intrusion Detection Approach (IDS). IDS present a second wall of defense. Intrusion detection method is needed to reactively detect attack to gain more time for improving the intrusion prevention method without resulting so many destruction in the network.

III. GRAY HOLE ATTACK

Gray hole attack is type of Denial of Service (DoS) attack. A Gray Hole Attack where attacker misleads the network by agreeing to forward the packets. When it obtain the packets from the neighboring node, the attacker drop the packets / messages. This is a kind of active attack. In gray hole attacking node initially consent to send packets and then fails to do so. Firstly the node acts perfectly and reruns accurate RREP messages to nodes that begin RREQ message. Like this, it get sending packets then the node now drops the packets to start a denial of service attack. This process goes on until malicious node is successful in its aim e.g. network resource consumption. The malicious behavior of gray hole attack is different in different ways. It drops packets while forwarding them in the network. In some other gray hole attacks the attacker node behaves maliciously for the time until the packets are dropped and then switch to their normal behavior [9]. Due this behavior it's very difficult for the network to figure out such kind of attack. This attack is also identified as routing misbehavior.

IV. RELATED WORK

F. Stanjano et al. presented [5] one of the most arising issues in MANET is the limited battery, attackers take an advantage of this flaw and tries to keep the nodes awake until all its energy is lost and the node go into permanent sleep.

Sergio Marti et al. [3] describe Different kinds of attacks have been analyzed in MANET and their affect on the network. Attack such as gray hole, where the attacker node behaves maliciously for the time until the packets are dropped and then switch to their normal behavior.

Nikos et al. proposed [2] the layered security approach that described and design criteria for creating secure ad hoc network using multiple authentication protocols are analyzed. The performance of several such known protocols, which are based on challenge–response techniques, is presented through simulation results.

P.V. Jani proposed [4] that MANET is very much popular due to the fact that these networks are dynamic, infrastructure less and scalable. Despite the fact of popularity of MANET, these networks are very much exposed to attacks.

A.Vani et al. presented [31] security issue is the main concern in AD HOC networks. The existing protocols are inadequate to discover various types of threats. To overcome this problem designing a new routing protocol to provide solution for detecting and preventing nodes from security threats. This paper proposed network security protocol includes with Intrusion detection system. It observe the network traffics and trying to investigate the misbehave activities like attackers, wormhole, anomalies, failure, channel blocked success plus other anonymous behavior in network and maintenance. The performance of the protocol is measured using packet delivery ratio, Average end- to- end delay, routing overhead and throughput.

V. DETECTION AND PREVENTION TECHNIQUES OF GRAY HOLE ATTACK IN AODV

In this paper, Gray Hole attack in wireless ad-hoc networks using AODV Protocol be simulated and evaluated its damage in the network. AODV is reactive protocol, when a node wishes to start transmission with another node in the network to which it has no route; AODV make available topology information for the node. AODV use control messages to discover a route for the destination node in the network. There are three types of control messages in AODV which are discussed bellow.

Route Request Message (RREQ):- This is a message used by AODV for the purpose of discovering new routes to a destination node. There is a time to live (TTL) value in every RREQ message, the value of TTL states the number of hops the RREQ should be transmitted.

Route Reply Message (RREP):-A node is having a requested identity or any intermediary node that has a route to the requested node produce a route reply RREP message back to the discoverer node.

Route Error Message (RERR):- Each node in the network maintains checking the connection status to its neighbor's nodes through active routes. When the node identifies a link break in an active route, (RERR) message is generated by the node in order to inform other nodes that the link is down.

Simulations done with the help of using NS-2 simulation program that consists of the collection of all network protocols to simulate many of the existing network topologies. Even though NS-2 contains wireless ad-hoc routing protocols, it does not have any modules to simulate malicious protocols. All routing protocols in NS are installed in the directory of "ns-2.35". Simulation Parameters used in this paper are mentioned below.

Number of Nodes	20
Communication Type	CBR
CBR Data Rate	10 Kbits
Simulation Area	750m x 750 m
Maximum mobility speed of	20 m/sec
Simulation Time	30 seconds
Packet Size	512 bytes
Number of Connections	10
Pause Times	1.0
Number of malicious nodes	0, 1,2
Transmission Speed	20 Mbps
Routing Protocol	AODV, grayholeAODV, idsAODV

Table 2 – Simulation parameters

The work is started by duplicating AODV protocol in this directory and changes the name of directory as "grayholeaodv". Names of all files that are labeled as "aodv" in the directory are changed to "grayholeaodv" in this new directory except for "aodv_packet.h". All classes, functions, structs, variables and constants names in all the files in the directory except struct names that belong to AODV packet.h code, have been changed.

AODV and grayhole aodv protocols have been designed to send each other aodv packets. After the above changes, the change has been made to two common files that are used in NS-2 globally to integrate new gray hole aodv protocol to the simulator In this implementation there is no need to add a new packet. Therefore only two files have been changed. The changes are explained below. The First file modified is "\tcl\lib\ ns-lib.tcl" where protocol agents are coded as a procedure. When the nodes use grayhole aodv protocol, this agent is scheduled at the beginning of the simulation and it is assigned to the nodes that will use grayhole aodv protocol. Second file which is adapted is "\makefile" in the root directory of the "ns-2.35". Till now, a new routing protocol have been implemented which is labeled as grayholeaodv. next modification in idsaodv.h is to declaire and define the RREP cache mechanism in the idsaodv.h file. To take accurate results from the simulations, UDP protocol has been used.

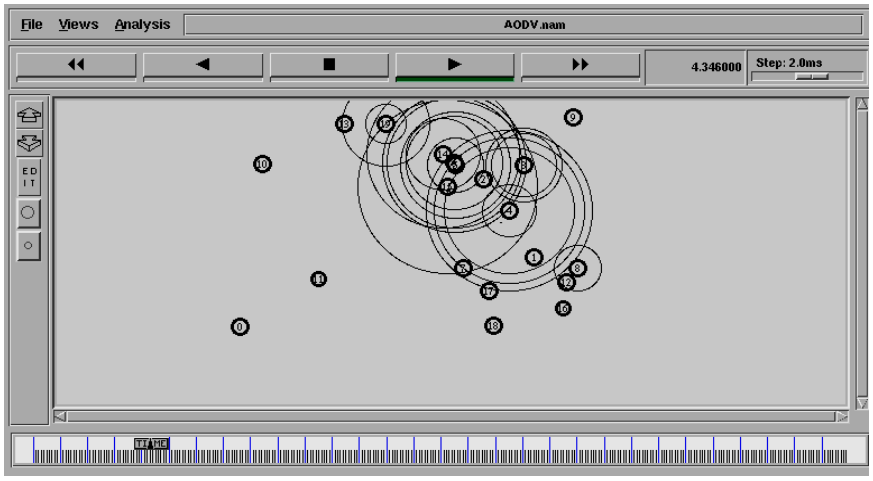

Figure 1 : Snapshot of the scenario for AODV and IDSAODV

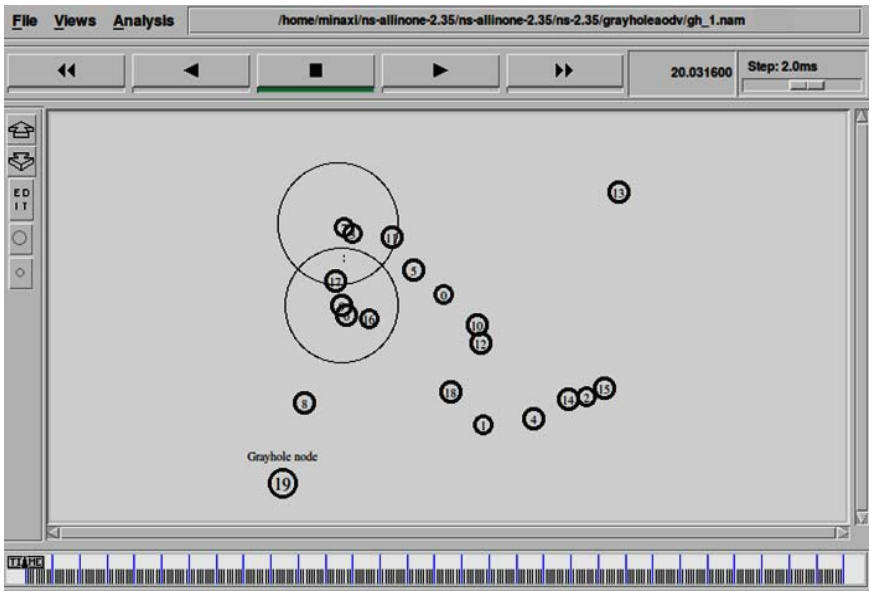

Figure 2 : Snapshot of the scenario for AODV with one grayhole node and IDSAODV with one grayhole node

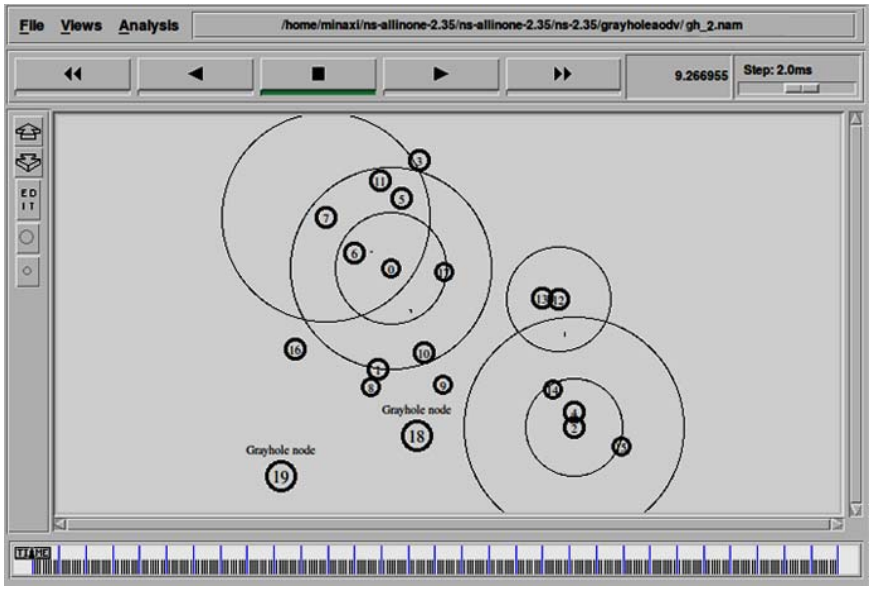

Figure 3: Snapshot of the scenario for AODV with two grayhole node and IDSAODV with two grayhole node

Above scenario shows that In Figure1 there are 20 nodes without any Grayhole node and the protocol used is AODV. In Figure2 there are 20 nodes with one Grayhole node (node 19) and the protocol used is idsAODV for trusted nodes (node 0 to node 18) and grayholeAODV for grayhole node (node 19). In Figure there are 20 nodes with two Grayhole node (node 18 and node 19) and the protocol used is idsAODV for trusted nodes (node 0 to node 17) and grayholeAODV for grayhole nodes (node 18 and node 19). In this paper, make an effort to evaluate the effects of these simulations to recognize the network and node performances. Initially calculate the packet loss. Therefore count how many packets are sent by the sending nodes and how many of them reached the receiving nodes.

VI. CONCUSION

In this paper, the effect of the Gray Hole in an AODV Network is analyzed. In this work three scenarios are simulated in which first simulation is without any gray hole node and second one is with one gray hole node and third one used two gray hole node. It has been tried to make an effort to evaluate the effects of these simulations to recognize the network and node performances First attempt is to evaluate the packet loss. Therefore we counted how many packets are sent by the sending nodes and how many of them reached the receiving nodes. In the previous section, we described how we obtain the numbers of the packets. After the analyzing the simulation result it is concluded that if a Gray Hole Node is introducing in this network data loss is increased to 10 % in presence of one gray hole node and increased to 20% in presence of two gray hole node in the network. As 3 % data loss already exists in this data traffic, Gray Hole Node increases this data loss by 7 % and 17% respectively. Even if idsAODV protocol is used in the same network, the data loss decreased to 45 % in case of one gray hole node present in the network and decreased to 52% in case of two gray hole nodes. These two results show that our solution reduces the Gray Hole effects by 15-17% as packet loss in a network using idsAODV .

REFERENCES

[1] Nital Mistry, Devesh C Jinwala and Mukesh Zaveri, “Improving AODV Protocol against Blackhole Attacks”,Proceeding of the International MultiConference of Engineers and Computer Scientists 2010 Vol II,IMECS 2010

[2] Nikos Komninos, Dimitrios D. Vergados and Christos Douligeris, “Authentication in a layered security approach for mobile ad hoc networks”, computers & security 26 (2007) 373–380.

[3] Sergio Marti, T.J.Giuli, K.Lai, M.Baker, “Mitigating Routing Misbehavior in Mobile Ad- Hoc Networks”, 6th ACM International Conference on Mobile Computing and Networking, August 2000.

[4] Ira Nath and Dr. Rituparna Chaki, “BHAPSC: A New Black Hole Attack Prevention System in Clustered MANET”, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 8, August 2012.

[5] P.V.Jani, “Security within Ad-Hoc Networks,” Position Paper, PAMPAS Workshop, Sept. 16/17 2002.

[6] F.Stanjano, R.Anderson, “The Resurrecting Duckling: Security Issuesfor Ubiquitous Computing,” Vol. 35, pp. 22-26, Apr, 2002.

[7] Y. Hu, A. Perrig, and D. B. Johnson, .Ariadne: A Secure On Demand Routing Protocol For Ad Hoc Networks,. in Proc. of MobiCom ’02, Atlanta, USA, Sept. 2002.

[8] D. Johnson, D. Maltz and J. Broch, “DSR the Dynamic Source Routing Protocol for Multihop Wireless Ad Hoc Networks”. Ad Hoc networking, Chapter 5, page 139- 172. Addison- Wesley, 2001.

[9] Sanjay Ramaswamy, Huirong Fu, Manohar Sreekantaradhya, John Dixon and Kendall Nygard, “Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks” Department of Computer Science, IACC 258,North Dakota State University, Fargo

[10] H. Yang, H Y. Luo, F Ye, S W. Lu and L Zhang, “Security in mobile ad hoc networks:Challenges and solutions”, IEEE Wireless Communications. 11 (1), pp. 38-47.

[11] A.Vani, and D.Sreenivasa Rao, “Providing of Secure Routing against Attacks in MANETs” International Journal of Computer Applications,Volume 24– No.8, June 2011