GH-AODV ROUTING TECHNIQUES TO DETECT AND PREVENT GRAY HOLE ATTACK IN MANET

M.Indhumathi, Dr.T.Ranganayaki

Abstract

One of the most critical problems in MANETs is the security vulnerabilities of the routing protocols. A set of nodes may be compromised in such a way that it may not be possible to detect their malicious behavior easily. Such nodes can generate new routing messages to advertise non-existent links, provide incorrect link state information, and flood other nodes with routing traffic, thus inflicting Byzantine failure in the network. In this paper, we discuss one such attack known as Gray Hole Attack on the widely used AODV (Ad hoc On-demand Distance Vector)routing protocol in MANETs. A mechanism is presented to detect and defend the network against such an attack which may be launched cooperatively by a set of malicious nodes.

Keywords: Gray hole, MANET, routing protocols, node

Introduction

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.

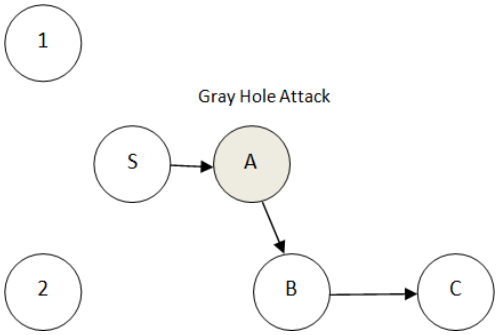

Figure 1: Gray Hole Attack

In this paper, GH-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 GH-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. GH-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 its 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.

GRAY HOLE ATTACK

Gray hole is one of the attacks found in ad hoc network. Which act as a slow poison in the network side it means we cannot suppose how much data can be lost. In gray hole attack a malicious node trashes to precede certain packets and simply drops them. The attacker selectively drops the packets originating from a single IP address or a range of IP addresses and forwards the remaining packets. Gray hole nodes in MANETs are very effective. Every node maintain a routing table that stores the next hop node information for a route a packet to destination node ,when a source node want to route a packet to the destination node , it uses a particular route if such a route is accessible in its routing table. If not, nodes initiate a route discovery process by broadcasting Route Request (RREQ) message to its neighboring nodes. By getting the RREQ message, the intermediate nodes bring up-to-date their routing tables in a reverse route to source node. A Route Reply (RREP) message is sent backward direction of the source node after the RREQ query reaches either the destination node itself or any other intermediate node that has a recent route to destination. Now we define the gray hole attack on MANET'S .The gray hole attack has two significant phases [4].

Related Work

Gupta [2015] proposed a new method RTMAODV (Real Time Monitoring AODV). It does not introduce any overhead. Moreover neighbor node detects and prevents Gray Hole attack using real time monitoring. The concept of broadcasting is being used in the method. Node which replies to Route Request (RREQ) by source is being monitored in promiscuous mode. Detection of malicious node is actually done by neighbor node of Route Reply (RREP) sender node i.e. suspected node [1].

Ranjan, Singh & Singh [2015] have focused on the Gray hole attacks. These Gray hole attacks poses a serious security threat to the routing services by attacking the reactive routing protocols resulting in drastic drop of data packets. AODV (Ad hoc on demand Distance Vector) routing being one of the many protocols often becomes an easy victim to such attacks. The survey also gives up-to-date information of all the works that have been done in this area. Besides the security issues they also described the layered architecture of MANET, their applications and a brief summary of the proposed works that have been done in this area to secure the network from Grey Hole attacks[2].

Gupta & Rana [2015] surveyed regarding the various kind of attacks happened on the network layer in MANET. The proposed scheme has been given for securing the network in malicious environment. In this source node will start the route discovery for data transfer like as AODV default process. In next step, all possible paths to reach destination in routing table and all information about the all path which is available for data transfer has been stored. Then the path having highest sequence number will be deleted from the routing table. Here they have deleted first two paths having highest sequence number and then the data will be sent to third highest path. They observed that throughput and end-to-end delay decreased in all three cases of attacks as simulation time increased [3].

Jain & Khuteta [2015] proposed a scheme in which they deploy the base node in the network that increases the probability of detecting multiple malicious nodes in network and further isolate them from taking part in any communication. In this procedure, Base Node sends dummy RREQ packet in network with the destination set as random generated network address that do not exist in the network, and it start timer and wait for replies from other nodes. Once the timer expires, it checks for the replies received from nodes. Genuine nodes do not send reply as the dummy RREQ is for node that do not exist in network [4].

Arya et al. [2015] instigate to detect and avoid the wormhole attack and collaborative Gray hole attack using trusted AODV routing algorithm. During the route discovery phase of the AODV Routing protocol, the trust value is also computed for all the neighbours of any node. To detect the malicious behavior of nodes, in this scheme each node maintains a Trust table. The Trust table has two columns. First the identifier or name of its entire neighboring node and second its relationship status with the neighbor node that could be Most Reliable, Reliable or Unreliable [5].

Chaube et al. [2015] have studied the impact of network size of their proposed Trust Based Secure On Demand Routing Protocol called "TSDRP" and AODV routing protocol for making it secure to thwart Gray hole attack. TSDRP protocol is capable of delivering packets to the destinations even in the presence of malicious node while increasing network size. In order to make result more accurate the performance of these two protocols TSDRP and AODV was tested with respect to different performance metrics and after observation of performance analysis, they concluded that in case of Gray hole attack TSDRP demonstrate better performance in almost all parameters: PDF, AED, AT and NRL as compared to AODV[6].

Abdelaziz et al. [2014] have analyzed all possible security attacks against ad hoc on-demand distance vector protocol, and they have given a detailed overview of each attack that can target the operation of this protocol. Particularly, they have focused on attacks that targets routing flow, such as flooding, Gray hole, wormhole, and rushing attacks. The presented analysis in this paper is potentially helpful for protocol designers to assess their designs, and for security researchers to validate their security mechanisms such as intrusion detection systems and trust management systems [7].

Parmar & Jethva [2014] analyzed behavior of black hole and gray hole attacks under AODV protocol and show the effects of both on network layer. They have also tested malicious behavior of AODV under above attacks using various performance parameters like throughput, packet delivery ratio, normalized network load and end to end delay using different simulation parameters. They also concluded that Grey Hole attack degraded the network performance in terms of packet efficiency and throughput and behavior of Gray hole was very difficult to judge because

sometime they acted as normal node but sometime they dropped selective packets[8].

Patel & Chawda [2014] reviewed the two most important and vulnerable attacks namely the Grey Hole and the Gray hole attacks. This paper shows how the performance of the network is degraded due to these two attacks. Many techniques to mitigate these attacks have been provided. Every technique has its own advantages and limitations which are also listed in the paper [9].

DETECTION AND PREVENTION TECHNIQUES OF GRAY HOLE ATTACK

In this article, Gray Hole attack in wireless ad-hoc networks using GH-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; GH- AODV make available topology information for the node. GH-AODV use control messages to discover a route for the destination node in the network. There are three types of control messages in GH-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.

Algorithm

Step 1. Network N consist of x_i number of nodes where x=1,2,…n
Step 2. **If**(source node 'S' wants to forward the packets to destination node 'Dest')
In ideal case where there exist no link/node failure during packet transmission
'S' selects the highest link quality path to route the data packets
For each (x=1; x<=n; x++)
Calculate PD % using $PD_x = packets_{received} - packets_{transmitted}$
If $(95\% \leq PD_x \leq 100\%)$
Then
Go to Step 3
Else if
Go to Step 4
End else if
End if
Else *During any node/link failure*
Second highest link quality path will be selected
End else
End if
Step 3. Node is idle and able to forward the data packets
Step 4. Node is grey hole affected node and the succeeding node will send an alarm message to its 2-hop preceding node to re-route the data packets through another path.

Simulation Setup

Parameter	Value
Simulator	NS - 2.3.5
Channel type	Wireless channel
Protocols	GH-AODV, DSR
Simulation duration	120 second
Packet size	512 kb
Traffic rate	128 bytes
Mobility Models	Random Waypoint
MAC Layer Protocol	802.11
Traffic Models	CBR
Network size	50 nodes
Topology	500 m x 500m

Result and Discussion

In this chapter, concentrates on the outcomes and the analysis is depends on the simulation executed on NS2 simulator. To evaluate the behavior of stimulated Grey-hole attack, considered the performance metrics of the packet delivery ratio, End-to-End delay and throughput.

Packet Delivery Ratio (PDR)

PDR is the ratio of the number of data packets received by the destination to the number of data packets sent by the source. The Figure 6 shows that PDR under Attack are very low. After Proposed IDS PDR ratio is going to increasing with compare to under attack.

Throughput

Throughput is the no. of data packets delivered from source to the destination per unit of time. In Figure 7 under Black hole attacks the throughput are near about 120 kbps when we are using proposed IDS system then its increasing.

No. of Nodes	Packet Delivery Ratio		Throughput		Average End to End Delay	
	GH-AODV	DSR	GH-AODV	DSR	GH-AODV	DSR
100	4.1	3.2	3.9	3.1	1.5	2.1
200	5.6	4.1	5.2	4.8	2.6	3.5
300	6.4	5.6	6.4	5.2	2.7	3.9
400	7.9	6.1	7.0	5.9	3.2	4.5
500	8.3	7.1	8.3	6.8	4.9	6.8

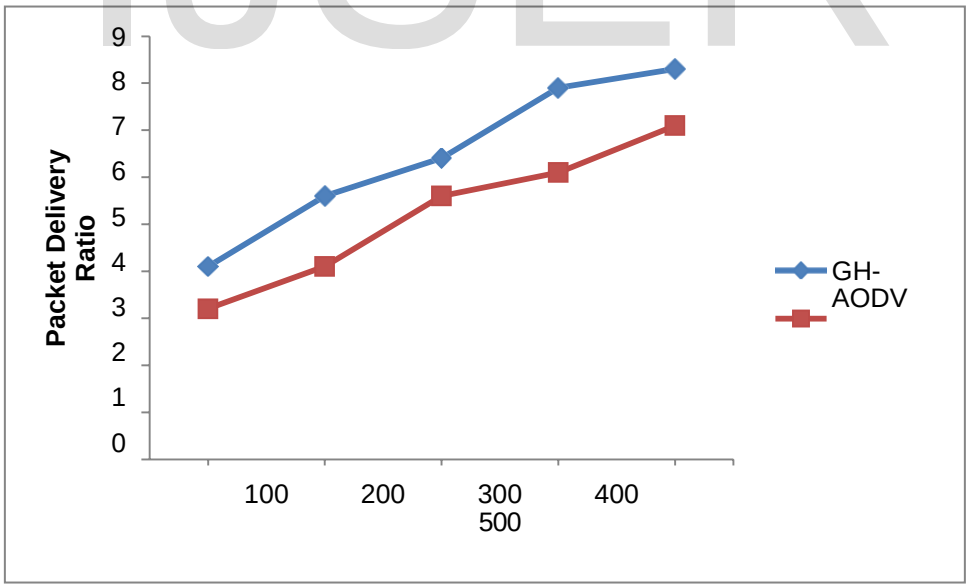

Figure 2: Packet Delivery Ratio

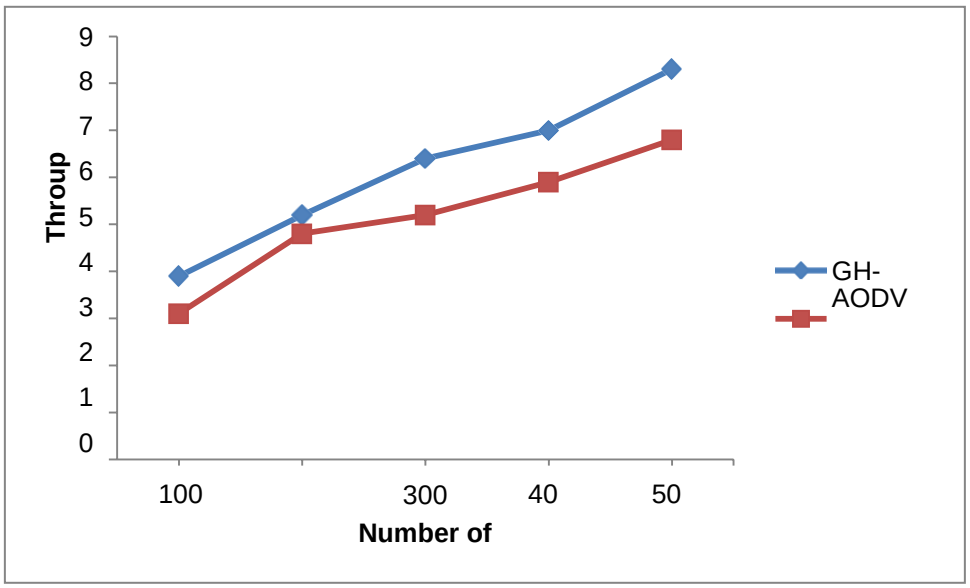

Figure 3: Througput

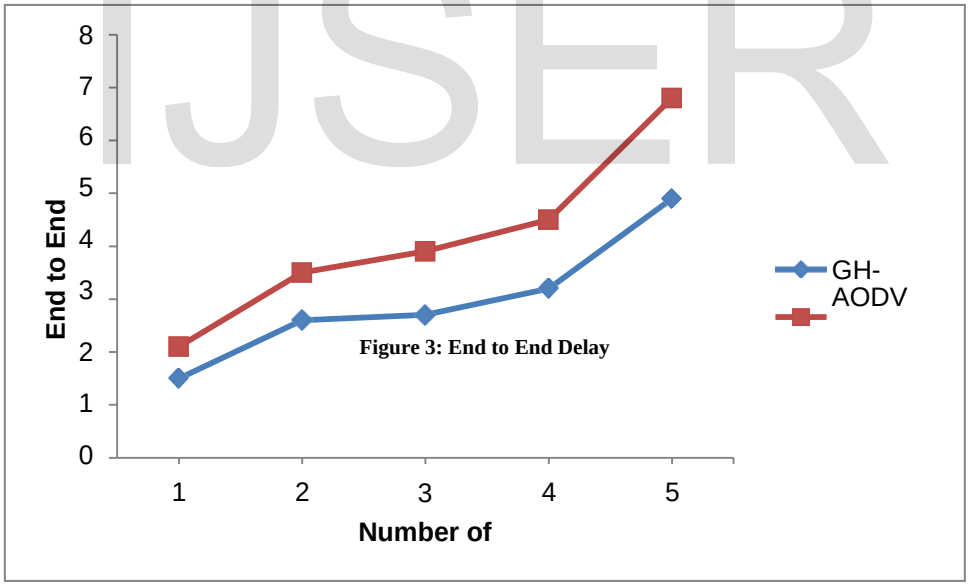

Figure 3: End to End Delay

Conclusion

MANET holds the possible to situate the network where a conventional network infrastructure environment cannot viable are situated. MANET is unlock to a variety of attacks. The destructive node creates the harm to the nodes and to the packets also. A new GH-AODV technique is used to detect and eliminate the gray hole attack in Network. In future work, the count of nodes used in the simulation process can be raised with the larger count of nodes. The harder is network, the more chance of occurrence of an attack. It is very important to prevent the attack in earliest stage otherwise it tends to lose all information which has to be sent to destination node. There can be more than one grey-hole attack in existence of one network.

References

1. Anurag Gupta,Kamlesh Rana, "Assessment of Various Attacks on AODV in Malicious Environment" 2015 1st International Conference on Next Generation Computing Technologies (NGCT-2015) Dehradun, India, 4-5 September 2015.
2. Sakshi Jain, Dr. Ajay Khuteta, "Detecting and Overcoming Grey Hole Attack in Mobile Ad hoc Network" IEEE 2015 International Conference on Green Computing and Internet of Things (ICGCIoT).
3. Neeraj Arya, Upendra singh, Sushma singh, "Detecting and Avoiding of Worm Hole Attack and Collaborative Grey Hole attack on MANET using Trusted AODV Routing Algorithm" IEEE International Conference on Computer, Communication and Control (IC4-2015).
4. Nirbhay Chaubey, Akshai Aggarwal, Savita Gandhi, Keyurbhai A Jani, "Performance Analysis of TSDRP and AODV Routing Protocolunder Grey Hole Attacks in MANETs by Varying Network Size" 2015 Fifth International Conference on Advanced Computing & Communication Technologies.
5. Amara korba Abdelaziz, Nafaa Mehdi, Ghanemi Salim, "Analysis of Security Attacks in AODV" IEEE 2014.
6. Martin K Parmar, Harikrishna B Jethva, "Analyse Impact of Malicious Behaviour of AODV under Performance Parameters" 2014 IEEE International Conference on Advanced Communication Control and Computing Technologies (ICACCCT).
7. Ankit D. Patel, Kartik Chawda, "Grey Hole and Gray hole Attacks in MANET" ICICES 2014 -S.A.Engineering College, Chennai, Tamil Nadu, India
8. 12. R.Rajeshkanna and Dr.A.Saradha " Multipath Load Balanced Congestion Control Routing Techniques in Mobile Adhoc Network", International Journal of Scientific Research and Development,Vol.2015 Issues 5, ISSN:2321-0613
9. 13. L. Pelusi, A. Passarella, and M. Conti, "Opportunistic networking: data forwarding in disconnected mobile ad hoc networks," IEEE Communications Magazine, vol. 44, no. 11, pp. 134–141, 2006.
10. 19. Shantharajah, S.P., Duraiswamy, Dr.K., Kadhar Nawaz, G.M., "Key management and distribution for authenticating group communication", 1st International Conference on Industrial and Information Systems, ICIIS 2006, pp. 133-137, 2006.