ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 6, June 2013

Analysis and Prevention of effects of gray hole attacks on Routing Protocol in Mobile Ad-hoc Networks

Bhimsingh Bohara[1],Varun Sharma[2]

Research Scholar, Computer Science, Amity University, Jaipur, India [1]

Research Scholar, Computer Science, Amity University, Jaipur, India [2]

Abstract— Mobile Ad hoc Networks also abbreviated as MANETs, are infrastructure less wireless networks which are characterized by dynamic topologies. MANET is made up of autonomous collection of users that are continuously on the move, over bandwidth constrained wireless links. Gray hole attack is an active kind of attack on adhoc networks where the attacking node first forwards packets and then later on drops the packets resulting in Denial of Service (DoS). As MANET being a network without any central administration, is vulnerable to such kind of attacks and network can be easily crippled by such malicious nodes. Therefore various kinds of security mechanisms are applied to protect networks from harm. Intrusion Detection Systems (IDs) are one of the solution which help in detecting the misbehaving node as well as notifies other nodes in networks of the misbehaving node. The main aim of security systems is to provide services like Authentication, Accountability, Integrity, Anonymity and Confidentiality. In this paper we have used AODV routing Protocol for route discovery. When malicious node starts dropping packets we use Intrusion Detection scheme to report violation of policy and the nodes whose packets are dropped again try to establish new paths using Route Requests (RREQ) messages. In our paper the NS2 scenario shows that the throughput is improved than traditional gray hole attacks.

Keywords-Ad hoc Network ,Network simulator NS-2,Security Threats, Grayhole Attacks, Routing Protocols,Performance, PDR, NRL,Packet Loss

I. INTRODUCTION

A Mobile Ad-hoc network (MANET) is an autonomous system of wireless mobile nodes without any fixed infrastructures. This kind of network promises many advantages in terms of cost and flexibility compared to network with infrastructures. MANET's are very suitable for a great variety of applications such as data collection, seismic activities, and medical applications. Unfortunately nodes in MANET are limited in energy, Bandwidth. These resource constraints pose a set of non-trivial problems in particular, routing and flow control [1].

Emergence of wireless network is in 1970 and it became popular in computing as well as communication industries. Mobile wireless network are of two types [2][8] infrastructure network and infrastructure less mobile network. In infrastructure less network nodes can move freely and make their own route with the help of topology and it may change rapidly according to time. Infrastructure less network is known as Ad hoc network. Mobile Ad hoc Network is a collection of mobile nodes in wireless technique. It never uses the existing network infrastructure and made its own temporary network. 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 state information, and flood other nodes with routing traffic, thus inflicting Byzantine failure in the network. In this work, 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 presented shows the method to detect & prevent from gray hole attack in Mobile ad hoc network [9].

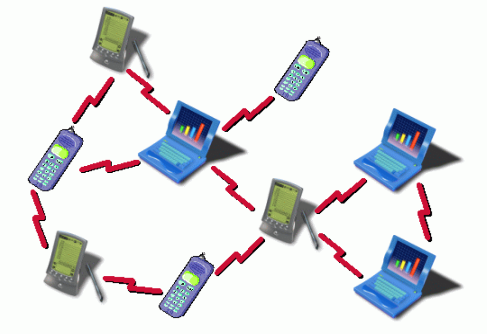

Figure1 [4] General Mobile Ad Hoc Network Architecture

It is an autonomous system, where nodes/stations are connected with each other through wireless links. There is no restriction on the nodes to join or leave the network, therefore the nodes join or leave freely. This property of the nodes makes the mobile ad hoc networks unpredictable from the point of view of scalability and topology.

In Mobile Ad hoc Networks the routing protocols are divided into following three categories.

1) Proactive
2) Reactive
3) Hybrid

The performance is measured by its routing protocols. Proactive protocol is a protocol which finds routes between all source –destination pairs regardless of the use or need for such route. Re-active protocols do not initiate finding routes unless it is required. Re-active protocols find their routes with the help of flooding query.

II. LITERATURE REVIEW AND RELATED WORK

S. Ramaswamy et. al. [10] presented an algorithm to prevent Collaborative Black hole attacks. The Algorithm was mainly based on Trust relationship between the nodes so it cannot tackle the problem of gray hole attacks. S Banerjee et. al.[11] have also proposed the algorithm to prevent Black/Gray hole attacks. Marti et. al.[12] also proposed watchdof algorithm to detect malicious nodes. In this Algorithm, when the node forwards packet the watchdog checks that the next node also forwards the packet by promiscuously listening to its transmissions. Madhavi S presented Intrusion Detection System for MANETs.

III. OVERVIEW AND ANALYSIS OF AD HOC ON DEMAND DISTANCE VECTOR PROTOCOL (AODV)

The Ad hoc On-demand distance vector routing [3] protocol based on Destination Sequenced Distance Vector (DSDV) protocol. It was introduced in 1997. AODV is designed for networks with ten to thousands of mobile nodes. One feature of AODV is the use of a destination sequence number for each routing table entry. The sequence number is created by the destination node. The sequence number included in a route request or route reply is send to requesting nodes. Sequence number are very important because they ensures loop freedom and is simple to program. Sequence numbers are used by other nodes to determine the freshness of routing information. If a node has the choice between two routes to a destination, a node is required to select the one with the greatest sequence number. When a node want to find route to another node it sends a RREQ to the entire network till either the destination is found or another node is reached. The RREP is sent back to the source and the search route is made available. When a node searches a route and found that this route is not valid then it removes entry from routing table and sends a RERR message to neighbours that are uses the route; this is possible by making an active neighbour lists. This procedure is repeated again and again at nodes that receive RERR messages. When a source receives an RERR then it reinitiate a RREQ message. AODV does not allow handling unidirectional links.

AODV deals with routing table. Every node has a routing table. When a node knows a route to destination, it sends a route reply to the source node.

It entries are Destination IP address, Prefix size, Destination sequence number, Next hop IP address, Lifetime(expiration or deletion time of route), Hop count(number of hops to reach the destination), Network interface , Other state and routing flags (e.g. valid, invalid) Route requests(RREQs), Route Replies(RREPs) and Route Errors(RERRs) are message types define AODV.

Let us take an example in which a node S wants to communicate with D Figure 2, the node sends a RREQ to find a route to the destination. S generates a Route Request along with destination address.

Sequence number and Broadcast ID and sent it to his neighbour nodes. Each node receiving the node request sends a route back (Forward Path) to the node.

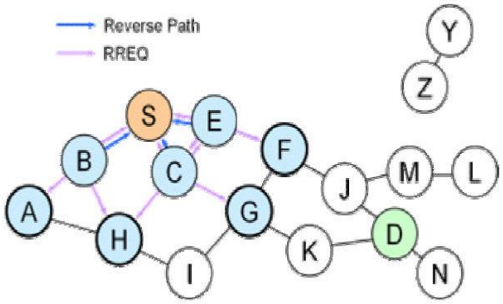

Figure 2[8]: Path finding in AODV

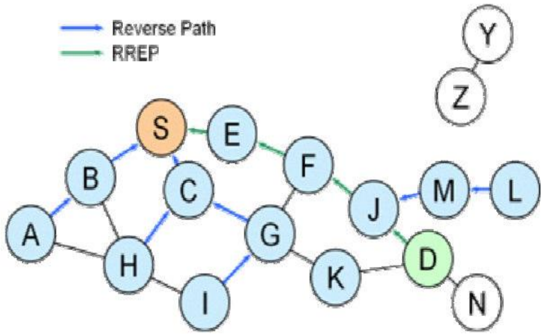

Figure 3[8]: Path finding in AODV.

Here in figure 3, 4 S can able to communicate with node D.

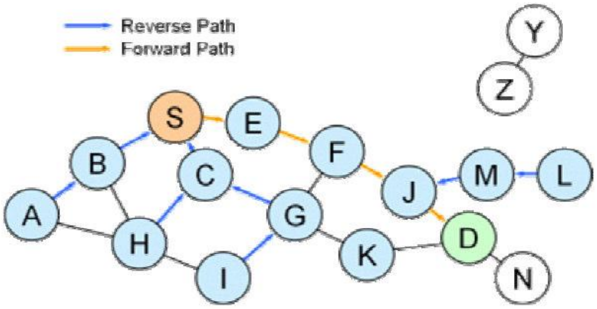

Figure 4[8]: Path finding in AODV

When a link break in an active route is detected, the broken link is invalid and a RERR message is sent to other nodes, Figure 5. If the nodes have a route in their routing table with this link, the route will be erased. Node S sends once again a route request to his neighbor nodes. Or a node on the way to the destination can try to find a route to D. That mechanism is called: Local Route Repair.

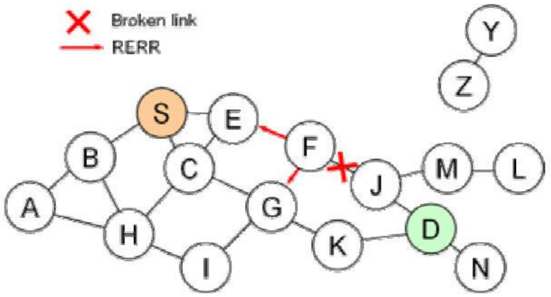

Figure 5[8]: Path finding in AODV

IV. ATTACKS ON MOBILE AD-HOC NETWORKS

Malicious or Misbehaving nodes are the ones creating attacks on physical, network, links as well as application layer. Current Routing Protocols mainly face two kinds of attacks.
Active Attacks which consist of Spoofing, Wormhole attacks, Sinkholes, Fabrication, Modification,DoS etc.
Passive Attacks consist of eavesdropping, Monitoring,etc.

*BLACKHOLE ATTACK*s:
In this kind of attack the misbehaving node falsely advertises shortest or good path to destination during path finding process . The main reason behind such malicious activity can be anything from interrupting data packets to disrupting path finding process. The mischievous node always advertises good path irrespective of its availability in routing table. In this way attacker node will always have the availability in replying to the route request and thus intercept the data packet and retain it[6]. In protocol based on flooding, the malicious node reply will be received by the requesting node before the reception of reply from actual node, fake route is established. When this route is established, now it's up to the node whether to drop all the packets or forward it to the unknown address [13]. The detection of Black hole attacks is though not tough as the malicious node either drops all the packet or sends to some other address.In this way either all data is lost or consumed.

GRAYHOLE ATTACKS:
This kind of attack is also called routing misbehaviour attack. The Gray hole attack is in a way bit similar to Black hole attack. A black hole attack where drops all the packets, on the other hand the gray hole attacking node drops packet with certain probability. In some other cases the misbehaving node drops interrupted packets for some duration and then again starts behaving normally. Such nodes are hard to discover in the network an can cause disruption in network without being detected[7].

SPOOFING: Spoofing occurs when a malicious node misrepresents its identity in order to alter the vision of the network topology that a benign node can gather.This kind of attack is also called man-in-the-middle attack.

IMPERSONATION: If the authentication mechanism is not properly implemented a malicious node can act as a genuine node and monitor the network traffic. It can also send fake routing packets, and gain access to some confidential information.

V. PERFORMANCE EVALUATION

A. Simulation setup

We have setup this by using Network Simulator NS-2 and investigate the performance of AODV under the influence of Grayhole Attack ie GH-AODV and IDAODV which is AODV after the inclusion of Intrusion Detection System and also have compared it with Routing Protocol AODV. First we have generated the scenario files by taking an area of 600m x 600m and divide them into two categories.

1. Fix Pause time (10 sec), Max Speed (20m/s) and Simulation Time (200 sec) constant and number of nodes may vary.

2. By varying the speed and number of nodes are fixed (30). Fix Pause time (2 sec) and Simulation Time (200 sec).

Every simulation was done for 200 seconds.

B. Metrics

a. Packet Delivery Ratio: Total number of delivered data packets divided by total number of data packets transmitted by all nodes. This performance metric will give us an idea of how well the protocol is performing in terms of packet delivery at different speeds using different traffic models.

b. Packet Loss: It is the measure of the number of packets dropped by the routers due to various reasons.

c. Average end-end Delay: Total number of routing packet divided by total number of delivered data packets.

d. *Throughput:* Throughput is the measure of how fast we can actually send through network. The number of packets delivered to the receiver provides the throughput of the network.

e. *Normalized Routing Load:* The Normalized routing load for any Routing protocol is calculated by computing the sent or forwarded control packets divided by number of data packets received.

Simulation Parameter	Value
Simulation Time	200 Seconds
Simulation Area	600m x 600m
Transferring Mode	Unicast
MAC Layer	802.11
Examined routing protocol	AODV, GH-AODV, ID-AODV
Mobility model	Random waypoint
Transmission Range	250m
Maximum Speed	5, 10, 15, 20,25 m/s
Pause time	10s
Traffic Type	CBR (UDP)
Maximum Connections	12
Payload Size	512 bytes
Packet rate	4 pkts/sec

Figure 6: Simulation Parameters

VI. Result Discussion

a. Packet Delivery Ratio: It tells about the number of packets delivered from the whole packets. So by our simulation result the following Figure 9 shows graph of packet delivery percent v/s Max. Speed. It is observed that the Packet delivery ratio degrades after the inclusion of gray hole node. But when improved AODV with Intrusion Detection is used the PDR improves.

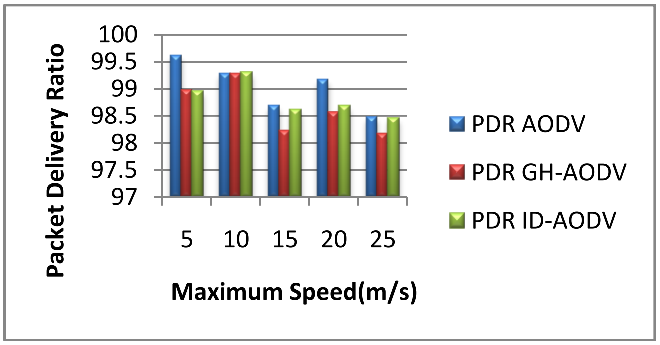

Figure 7

b. Average end-end delay:. Performance is overhead when end to end delay is maximum. From our simulations we can observe that the e-e delay for normal AODV is minimal even at varying speeds. But it increases under Attack and that is shown as Red Bar in the following Graph (Figure 8).And the result shows that it is reduced after including Intrusion Detection scheme in AODV.

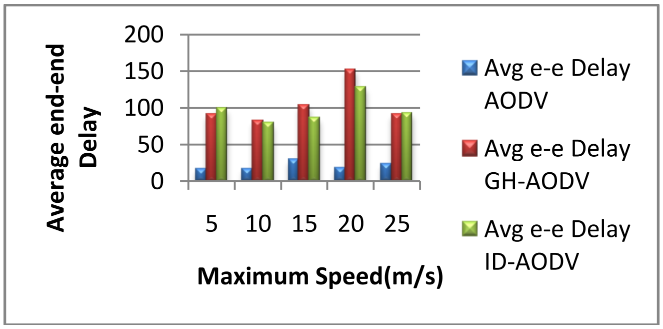

Figure 8

c. Throughput: It is seen from our simulations that normal AODV routing protocol outperforms in terms of throughput without being under the influence of Gray hole attack. At varying speeds network when being under attack and also when prevented from attack by Intrusion detection, gives almost same throughput. Figure 9 represents variations in throughput.

.

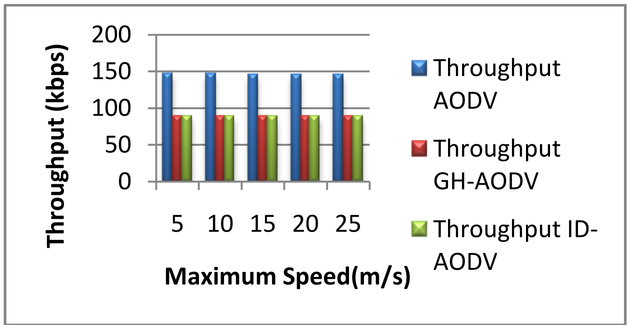

Figure 9

d. Packet Loss: The number of packets dropped by routers is called packet loss. Here our simulations shows that the packet loss is more when network is under attack by malicious node. There is slight improvement ie. Reduction in packet loss when solution ie IDAODV is introduced.

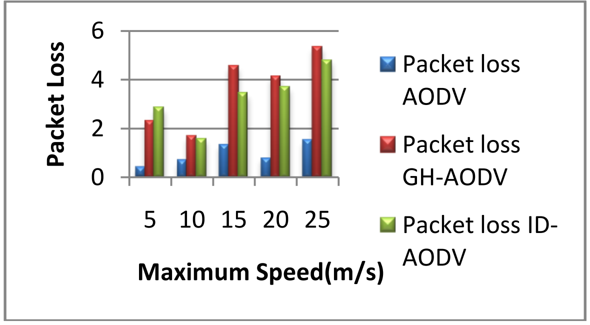

Figure 10

e. NRL: This is one of the crucial metric in understanding the delay introduced by path discovery. The Graph shows the Normalized Routing Load. The Routing Protocol behaves almost same in all conditions as the packet delivery percent is quite high in this scenario.

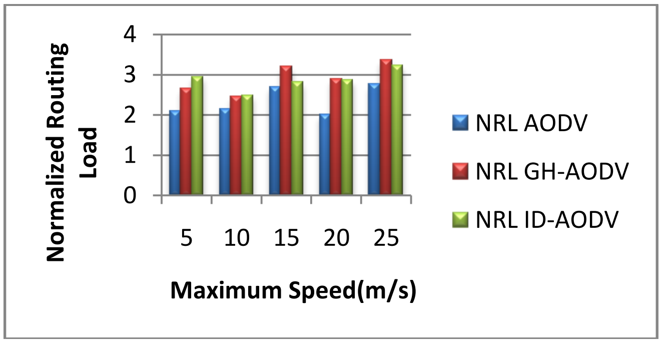

Figure 11

VII. CONCLUSION

Misbehaving nodes or Malicious nodes can cause severe damage to the network if not taken care of. In this paper we have implemented the gray hole attack and also showed that Intrusion Detection can be helpful for detecting such attacks.

In this paper we analyzed the effects of gray hole in an AODV network. For this purpose, we modified and implemented AODV protocol that behaves as gray hole in NS-2. We took simulation results with varying speed and 30 nodes for normal AODV as well as after the inclusion of gray hole in AODV. From our simulations we can easily see that normal aodv had very less data loss (4.16%)but after including the malicious node the data loss increased drastically(91.04%). When we used the solution for GHAODV ie. IDAODV in the same network The data loss again decreased (85%).We also observed that the throughput of normal AODV was much better compared to gray hole and its solution. As the speed varied the average end to end delay remained almost same for normal behavior of AODV but the malicious node in AODV increased the e-e delay too much which was then brought to normal by our Solution.

REFERENCES

[1] E. M. Royer and T. Chai-Keong, "A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks," *Personal Communications, IEEE, vol. 6, April 1999, pp. 46-55.*

[2] NS-2, the NS Manual. Available at http://www. isi.edu/nsnam/ns/doc.

[3] C.E. Perkins and E.M Royer, "Ad Hoc On-Demand Distance Vector Routing", *Proc 2nd IEEE Workshop Mobile Comp. Sys and Apps., New Orlean LA, Feb 1999, pp. 90-100*

[4] A.Pravin Renold,"Source based Trusted AODV Routing Protocol for Mobile Ad hoc Networks"*ICACCI-2012*.

[5] Y. Hu, A. Perrig and D. Johnson, Ariadne: A Secure On-demand Routing Protocol for Ad Hoc Networks, in Proceedings of ACM MOBICOM'02, 2010.

[6] G. A. Pegueno and J. R. Rivera*, "Extension to MAC802.11 for performance Improvement in MANET",* Karlstads University, Sweden, December 2006.

[7] L. Zhou, and Z. Haas, "*Securing ad hoc network*," IEEE Network Magazine, Special issue on network security, Vol. 13, No. 6, November/December 1999, pp. 24-30.

[8] Goel and Anjali Sharma," Performance Analysis of Mobile Ad-hoc Network Using AODV Protocol*" (IJCSS), Volume (3): Issue (5).*

[9] K. Snazgiri, B. Dahill, B. Levine, C. Shields, and E.A.Belding-Royer, "*Secure routing protocol for ad hoc networks*," In Proceedings of International Conference on Network Protocols (ICNP), Paris, France, November 2002.

[10] Sanjay Ramaswamy, Huirong Fu, Manohar Sreekantaradhya,John Dixon, and Kendall Nygard, "Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks". In Proceedings of 2003 International Conference on Wireless Networks (ICWN'03), Las Vegas, Nevada, USA, pp. 570-575.

[11] Sukla Banerjee "Detection/Removal of Cooperative Black and Gray Hole Attack in Mobile Ad-Hoc Networks" Proceedings of the World Congress on Engineering and Computer Science 2008 WCECS 2008, October 22 - 24, 2008, San Francisco, USA

[12] S. Marti, T. J. Giuli, K. Lai, and M. Baker, Mitigating Routing Misbehavior in Mobile Ad Hoc Networks. *Proceedings of the 6th annual international conference on Mobile Computing and Networking (MOBICOM)*, Boston, Massachusetts, United States, 2000, 255-265.

[13] K. Biswas and Md. Liaqat Ali, *"Security threats in Mobile Ad Hoc Network",* Master Thesis, Blekinge Institute of Technology" Sweden, 22nd March 2007.