Indian Journal of Science and Technology, Vol 9(47), DOI: 10.17485/ijst/2016/v9i47/106451, December 2016
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Detection and Avoidance of Gray Hole Attack in Mobile Ad-Hoc Network

Monika Angu* and Sami Anand

Department of Computer Science and Engineering, Lovely Professional University, Phagwara - 144411, Punjab, India; monikaangu@yahoo.com, sami.16840@lpu.co.in

Abstract

A MANET (mobile ad hoc network) might be called as a base less dynamic system which is a bunch of autonomous number of mobile nodes that can speak with each other utilizing radio wave. It is a self-designing system, where less systems of cell phones are associated by wireless. The arrangement of wireless gadgets called wireless nodes, which consequently interface and exchange data. Each hub in a MANET is allowed to move autonomously, and will in this manner change its associations with different gadgets often; each must forward activity inconsequential to its own utilization, and along these lines be a switch. The MANET system empowers customers and servers to impart in a non-settled topology region and it's utilized as a part of an assortment of utilizations and quickly developing systems .The technique used in the detection would increase the throughput and decrease the delay and packet loss. The method empowers our network strength and reliability.

Keywords: AODV, Different Attacks, Gray Hole Attack, MANET

1. Introduction

The development in the mobile gadgets (e.g., PDAs, portable workstations, individual computerized aides, or wearable PCs) and communication registering innovation are changing our method for sharing data. We are at the passage of the universal communication period which a client uses various gadgets through which they can get to all the required data at whatever point and wherever required. The omnipresent communication advocates wireless systems as the right arrangement and as an outcome, the wireless systems administration has experienced exponential development in the previous couple of decades.

A MANET (mobile ad hoc network) might be called as a base less dynamic system which is a bunch of autonomous number of mobile nodes that can speak with each other utilizing radio wave. It is a self-designing system, where less systems of cell phones are associated by wireless. The arrangement of wireless gadgets called wireless nodes, which consequently interface and exchange data.

The core problem of wireless ad hoc networks is routing data from sender to receiver through dynamic nodes. Since

It is an ad hoc network so cooperation of nodes is very important in order to establish network the prominent path is needed, if nodes which are not within that communication range will be establish through a multihop links in which it is responsibility of neighbor nodes to shift data packets from source to destination and destination to source.

An ad hoc network has dynamic nature due to which nodes changes their location as people keep on moving carrying that network. Nodes have freedom to join and leave the network whenever they need and shift to switch off mode when they wish to save the power and again shift to on mode when they wish to interface again. These type of network are very easy to deploy and cost effective.

In proposed work the main focus is on Ad hoc On–Demand Distance Vector (AODV) routing protocol which could be a unambiguously named on interest detachment vector routing protocol that develops path to

*Author for correspondence

the destination once it's searched for by the supply center point. It keeps up these routes as once needed by the supply center purpose. It offers fast assignment to element be part of conditions, low prepare process, memory overhead, low framework use, and chooses unicast route to the destinations within the impromptu system.

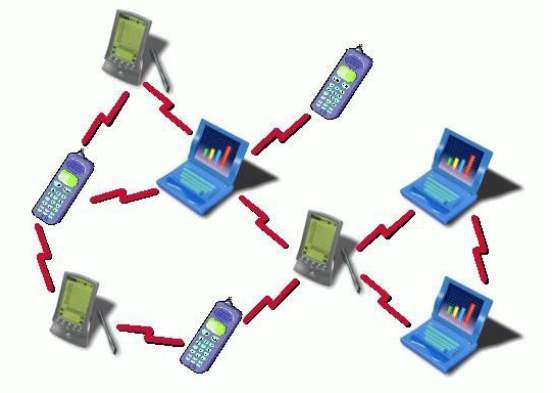

Figure 1. Mobile Ad-Hoc Network.

Three management packages that uses some messages such as Route Request (RREQ), Route Reply (RREP), Route Error (RERR) messages. AODV convention does not give a complete perspective of system topology to the nodes. In AODV convention every node just thinks about just its neighbors. AODV convention is not a safe convention in MANET. The security of AODV convention is bargained because of nearness of the vindictive hubs in the system. The pernicious node can be a Black hole and also in addition it can be a Gray hole node.

The standard AODV convention can't recognize vindictive node in the system because of its tendency of finding the new path to destination each time a source solicitation to exchange the information parcels (data packets).

2. Types of Attacks

There are many problems that leads to insecurity of MANET networks like no central control, limited bandwidth, easy eavesdropping, so MANET are more susceptible to attack than any other network. There are attacks which can be divided in network- layer attacks Passive, Active, Internal, External and Routing attacks and Packet forwarding attacks.

Active attacks embody actions such modification of information, replication information and deletion of changed data over the network. Sure active attacks is simply performed against an ad hoc network. These attacks is sorted in DoS, Impersonation revealing attack. Active attacks disturb the operations of the network and may be therefore severe that the complete network is brought down or degrade the network performance

Passive attacks include only the network and information monitoring. It involves tracing down the packets and getting the information presented inside them. Passive attacks mainly steal the data moving on the network and monitor the traffic pattern over the network. These activities are no performed on the network; they are tough to trace or identify.

The two common attacks are eaves dropping and traffic monitoring. An attacker can launch an attack against the network, to have enough information about that network that it can easily hijack and inject attack in the network.

If the proper security is not given to MANET network, it would lead to unwanted activities in the network. It is responsibility of the network to provide the objectives of network like confidentiality, availability, integrity, authentication, accountability. Due to this security is the major concern of MANET network.

3. Gray Hole Attack in Detail

A gray hole attack is a variation occurred in black hole attack, in which the promiscuous node is not initially malicious, what turn into malicious when needed. The predication of gray hole node is very difficult because of its random change of nature.

Grayhole is especially found in AODV routing protocol case in MANET. In Grayhole attack, the assaulter misleads the opposite nodes within the network by agreeing to forward the packets within the network. As shortly because it receives the packets from its neighboring node, the assaulter additional drops the packets. Grayhole is classed as a full of life attack. Grayhole node could be a node that by

selection drops the packets and simply forward the information packets, at that time it simply advertises itself as having the shortest path to destination node in response to the route request message.

In AODV protocol each mobile node maintains a routing table that stores the data of subsequent hop node for a routing a packet to a destination route.

It uses specified route, if such a route is accessible in its routing table else the node additional initiates a discovery method by the method of broadcasting a route request message to any or all its neighbors. Grayhole has two phases:

Gray hole attack has got two phases:

In the First phase, a compromised node tries to take advantage of the specifications in AODV protocol to advertise itself as having a sound route from supply to the destination node with a wrong intention of sniffing the packet despite the fact that the route is spurious.

In the Second phase the malicious node drops the intercepted packets supported an exact chance condition.

Grayhole attack will act as a slow poisoning within the network meaning we tend to cannot say that a hard and fast chance of information is lost. Grayhole attack is that the variation of part attack during which the node drops packets by selection (dropping on UDP packets and forwarding the TCP packets) or drop packets in applied math manner.

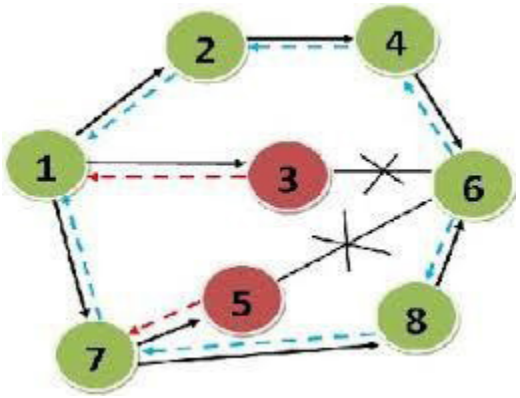

Figure 2. Gray hole attack in AODV.

4. The Research Methodology

Grayhole node drops the selective data packet. Here our work is to prevent the grayhole attack in the network as well as the

black hole attack. The approach being used is dropping of the node that reaches the threshold probability of packet drop. Through this approach the detection of grayhole node would increase.

The grayhole node selectively drops the packets in network. The malicious node in the grayhole attack is unpredicted because it only forwards the packet of TCP and drops UDP/FTP packets. In this approach we will use TCP and UDP/FTP packets that would be transferred through the network to detect the malicious node in the network.

Suppose we are using the AODV for the selection of the path from the source to destination and their exit the grayhole attack in the network. We will use the TCP and FTP protocol for the transmission of the data packets from one node to another node. We will propose our work with different number of node with different scenario.

The procedure would be followed as below:

- Source node will start transmitting the packets to the destination node.
- Firstly, the TCP packets would be forwarded or broadcast to the neighbor nodes through the path decided.
- As the TCP packets are forwarded by the gray node so there would be no loss of packet in this case and the source would get the positive acknowledgment from the destination and the intermediate node.
- Secondly, the TCP and FTP packets would be send by the source node.
- It will forward the TCP packets, but if the promiscuous node exists in the network it will drop the FTP packets.
- The detection of the malicious node would be detected by the ACK send by the destination and the intermediate node, if any node does not reply then the respective node would be considered as promiscuous node.
- This step would be repeated till the probability of the promiscuous node reaches to 60% that would indicate the probability of the gray node in the network.
- As the node reaches this value of probability the gray node would be dropped from the routing table

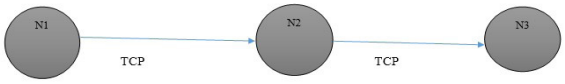

Figure 3. TCP data flow in Gray Hole attack.

5. Experimental Work

In the experimental work the simulation has been performed using NS2 network simulator tool. The different

scenario is simulated that provides us different graphs and output results to compare our study to the previous one. The n number of nodes are examined under normal network environment and under the malicious environment that provides with different values on the graph of throughput, packet loss and d e l a y .

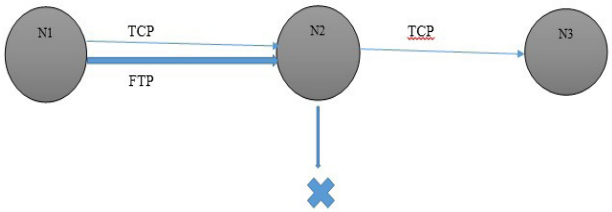

Figure 4. Dropped FTP packet in Gray Hole attack.

To prevent the Grayhole the approach used will be using some threshold value of new field called probability that would need to trusted network and the less packet loss and less packet-delivery ratio of the network.

Table 1. Simulation Parameter

Network	Wireless
Antenna	Omni Directional
No of nodes	12
MAC Type	802.11
Routing Protocol	AODV

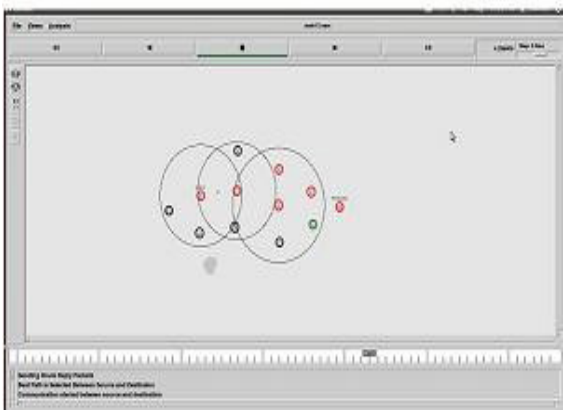

Figure 5. Nodes under Normal Network.

The figure 5 represents the nodes under the normal network when there is no malicious activity in the network. The normal AODV protocol could work and the route would be established.

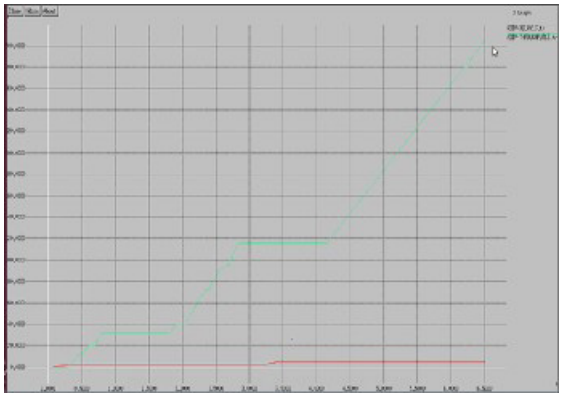

Figure 6. Graph of Throughput and Delay under Normal Network/

The throughput is explained as number of packets send by the sender in per unit of time. This is the main factor of performance evaluation of particular network. On the delayis term that specify how long it take a bit of data to transfer from one node to another .It is important design parameter for performance characteristics of computer networks. The graph above shows the linear growth of delay under normal network.

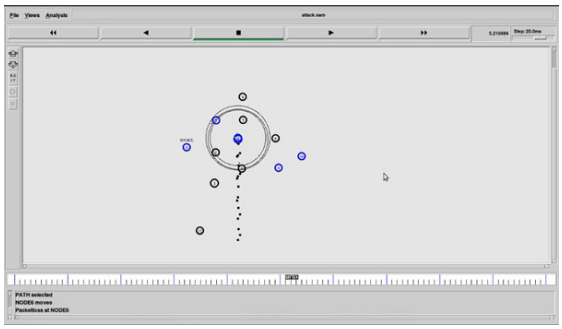

Figure 7. Network of nodes under attack.

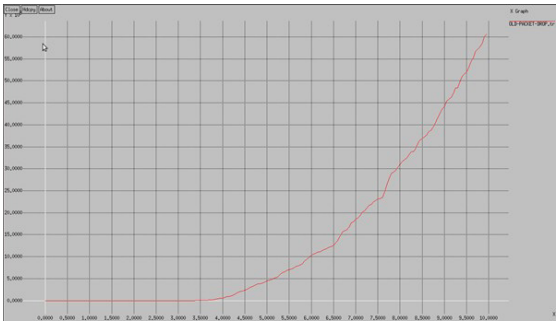

Figure 8. Graph of Packet Loss under Attack.

The figure above shows the network under the attack. It show the dropping of packet because of malicious activ-

ity. There is greater loss of packet, more delay and less throughput in the network under attack

The figure above show the packet loss in network under attack. The ration of packet loss increases, as the marginal line show the tremendous growth.

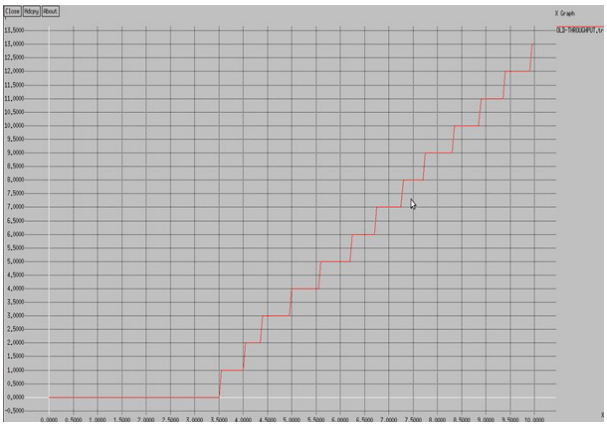

Figure 9. Graph of Throughput under attack.

The figure above show the output of throughput under attack

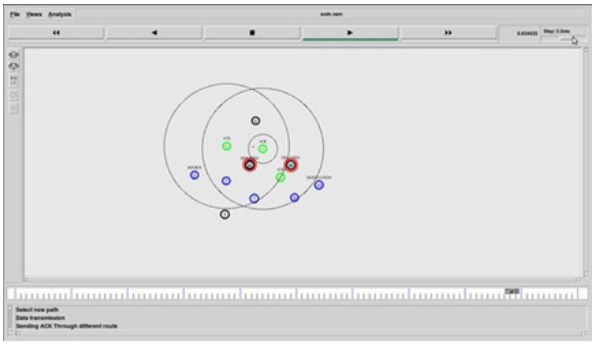

Figure 10. Mitigation the Attack.

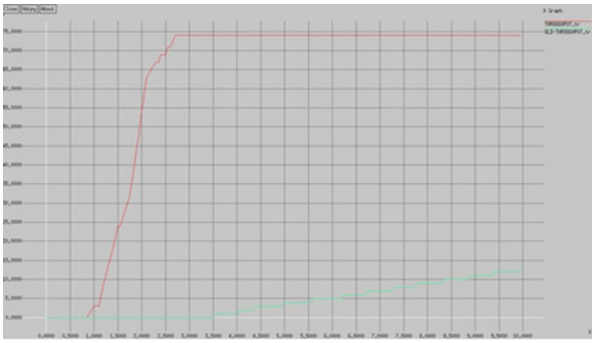

Figure 11. Combined Graph of Throughput under Different Network.

The figure above shows the defend against the attack in the network. The attack is defended by new algorithm and the new path is find for sending the packet from the source to destination.

The figure above show the throughput of network under attack and network when defended against the attack. The red marginal line shows the throughput after defend against the attack which gives the higher ration in graph on other way green line show the throughput under the attack that have very low throughput.

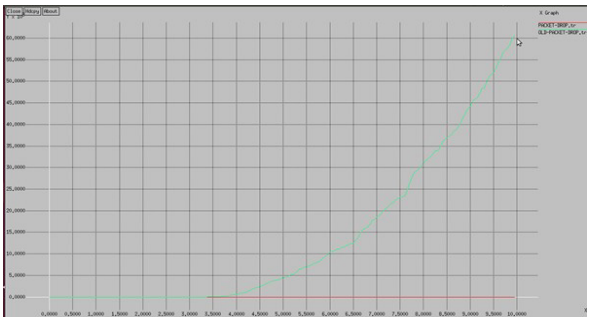

Figure 12. Combined Graph of Packet Loss under different network.

The above figure shows the combined ratio of packet loss in different environment.

6. Conclusion

In this work firstly the general working of MANET is summarized with the continuity of explanation about AODV in MANET. The different attacks have been explained with the different problems arising due to that attacks. In this work there is overall study of Mobile Ad Hoc network, its challenges with the further study of different attack available in Mobile ad hoc network that hampers overall performance of network

The simulation results depict that the method is efficient with high detection rate. Hence, significant research effort is needed prior to end up increasing the performance of network. Protocol implementation and practically building of test beds are crucial to understanding the performance and practicality issues.

In the future work the proposed scheme could be stimulated using other tool and could work on other parameters such as good put. In present section scheme there will be some delay but our prime focus would be on preventing the gray hole attack in the MANET network.

7. References

1. Basarkod PI, Manvi SS, Albur DS. Mobility Based Estimation of Node Stability in MANETs. Proceeding - IEEE International Conference on Emerging Trends in Computing, Communication and Nanotechnology. 2013.
2. Yang H, Luo H, Ye F, Lu S, Zhang L. Security in mobile ad hoc networks: Challenges and solutions. Proceeding - IEEE Wireless Communications. 2004 Feb.
3. Garg N, Mahapatra RP. MANET Security Issues. Proceeding - IJCSNS International Journal of Computer Science and Network Security. 2009 Aug; 9(8).
4. Ullah I, Ur Rehman S. Analysis of Black Hole Attack on MANETs using Different MANET Routing Protocols. Proceeding- Electrical Engineering thesis no: MME 10:62, 2010 Jun.
5. Wu Y, Mármol FG, Al-Duba A. Introduction to advances in trust, security, and privacy for wireless networks. In Proceeding- Wu et al. EURASIP Journal on Wireless Communications and Networking 2013. 2013; 287.
6. Jain S, Shastri A, Chaurasia BK. Analysis and Feasibility of Reactive Routing Protocols with Malicious Nodes in MANETs. In Proceeding- International Conference on Communication Systems and Network Technologies. 2013.
7. Ghosekar P, Katkar G, Ghorpade P. Mobile Ad Hoc Networking: Imperatives and Challenges. Proceeding - IJCA Special Issue on Mobile Ad-hoc Networks. 2010.
8. Rathod JJ, Lathigara A. Novel Approach of Preventing and Detecting Grayhole Attack on AODV based MANET. In Proceeding- International Journal of Advance Research in Computer Science and Management Studies. 2015 Jan; 3(1).
9. Kaur H, Sahni V, Bala M. A Survey of Reactive, Proactive and Hybrid Routing Protocols in MANET: A Review. In Proceeding- (IJCSIT) International Journal of Computer Science and Information Technologies. 2013; 4(3).
10. Sehgal E, Garg S. Mobile Ad hoc Networks (MANETs): Challenges, Applications and Security Goals with Minute Introduction of Routing Protocols. In Proceeding Internationals JARCSE. 2013 Aug; 3(8).
11. Balachandran A, Voelker GM, Bahl P. Wireless Hotspots: Current Challenges and Future Directions. In Proceeding -Mobile Networks and Applications. 2005; 10:256–74.
12. Jain J, Fatima M, Gupta R, Bandhopadhyay K. Overview and Challenges of Routing Protocol and Mac Layer in Mobile Ad-hoc networks.
13. Kong J, Hong X, Gerla M. A New Set of Passive Routing Attacks in Mobile Ad Hoc Networks. In Proceeding- IEEE MILCOM. 2003.
14. Yau P-W, Mitchell CJ. Security Vulnerabilities in Ad Hoc Networks. In Proc of the 7th Int Symp On Communications Theory and Applications. 2003; 99–104.
15. Aware AA, Bhandari K. Prevention of black hole attack on AODV in MANET- A survey. National conference on advances in computing, networking and security (NCACNS-2013)