International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2016): 79.57 | Impact Factor (2017): 7.296

Detection & Prevention of Gray Hole Attack in Mobile Ad-Hoc Network using AODV Routing Protocol

Siddharth Gupta[1], Skand Singh[2], Suramya Tripathi[3], Manish Kumar[4]

[1, 2, 3]Final Year Student, Department of CSE, Galgotia College of Engineering & Technology, Greater Noida, India

[4]Assistant Professor, Department of CSE, Galgotia College of Engineering & Technology, Greater Noida, India

Abstract: ***In this paper, we describe the basic idea related with the implementation of AODV protocol & impact of gray hole attack on adhoc network. Information exchange in a network of mobile and wireless nodes without any infrastructure support such networks are called as adhoc networks. They use wireless network connections to connect to various networks, capable of autonomous operation. Gray hole attack is the type of active attack in which as soon as the packet is received from the neighbour by showing itself having the shortest path to the destination node and the attacker drops the packet. Hence the data packets do not reach the destination node, data loss occurs. In this study, detection of the grayhole attack. As the behaviour of the attacker changes from malicious to normal after dropping the packet. This work shows the impact of the gray hole problem in the manet and the enhancement of the detection of the gray hole attack using RREQ & RREP approach.***

Keywords: NS-2, Gray Hole Attack, AODV Security threats, Packet forwarding misbehavior, adhoc network

1. Introduction

Mobile Ad Hoc Network is one of the most essential wireless network structures. All the nodes are moveable and has changing topology in adhoc network. Security is the essential service to wireless service networks. Manet is the network where the network is formed without the central administration. It contain mobile node which is used to send the packets[1,2]. In this work we will show the attack of the Gray hole attack. A way to detect and prevent the packet drop from the malicious node. Routing protocol plays a very important role in maintaining flawless communication between nodes which are quite apart from each other. Network topology was discovered with the help of routing protocol. Routing protocol does permit the route for transferring data packets and keeps the record of every transaction ever made.

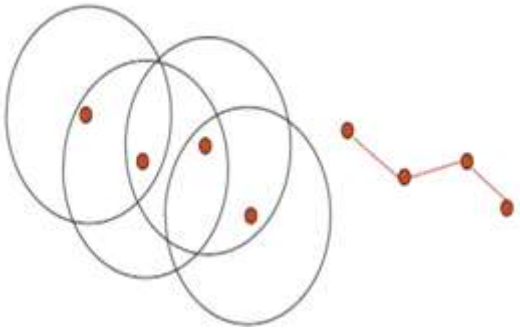

Figure 1.1: Representation of Wireless Network

1.1 Attacks on Mobile Ad-hoc Network

Attacks on mobile ad hoc networks can be classified into following two categories: passive attacks and active attacks.[4,5]

Passive attacks: A passive attack does not disrupt proper operation of the network.

Active attacks: An active attack attempts to alter or destroy the data being exchanged in the network, thereby disrupting the normal functioning of the network.

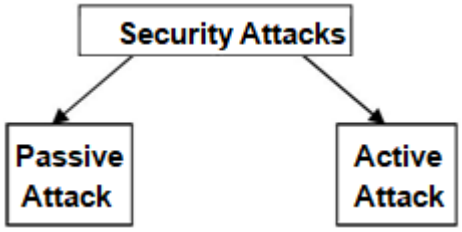

Figure 1.2: Attacks on Mobile Ad-hoc Network

Table 1.1: Attacks on mobile ad-hoc network

Passive Attacks	Active Attacks
Snooping, Eavesdropping, Traffic analysis	Worm hole, Black hole, Routing attacks

2. Basic Theory

2.1 GHA (Gray Hole Attack)

It is an attack on the adhoc network. In this type of attack the probability of loosing the data can't be predicted. In this attack [6] the maliciously node instead of forwarding the packets ,it drops them. The Gray Hole nodes in MANET are very useful. Each node maintains a routing table which has the next hop node information to send the packet to the destination node. Sometimes nodes gives a route discovery process message (RREQ) Route Request to it's neighbours. . On receiving this process message the intermediate nodes update their routing tables in order to reverse route to the source node. A Route Reply(RREP) message signal is given to the source node when the RREQ query reaches the destination node. The Gray Hole Attack consists of two stages[7], In the first stage the malicious node pretends to

have a valid route to the destination node thereby exploiting the AODV protocol. Whereas in the second stage node drops the interrupted packets. There are some other types of gray hole attacks in which the attacker node behaves maliciously until the packets are dropped and then changes into their normal behaviour. The other name of Gray hole attack is the node misbehaving attack.

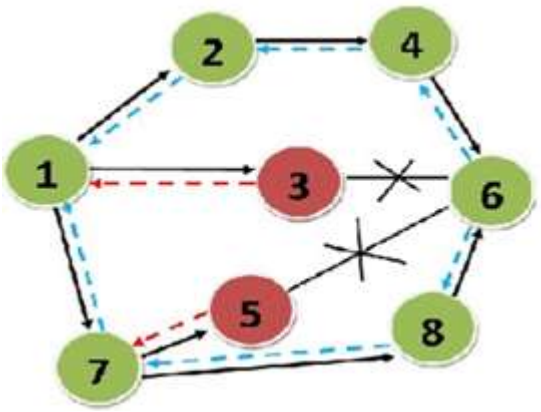

Figure 2.1: Gray hole attack in MANET

2.2 AODV Protocol in Manet

Routing attacks AODV stands for the Ad-hoc on-demand Distance Vector Routing protocol. It is built on the demand routing algorithm. The protocol consists of two operating functions route discovery and route maintenance .In and out of the beginning all the nodes send hello messages on its interface and simultaneously receives hello messages from its neighbours. This process is repeated periodically in order to determine neighbour connectivity .It uses two terms route request and route reply.

2.3 Performance Metrics

The performance of the network is analyze accord-ing to the following performance metrices :

Packet Delivery Ratio (PDR): It is defined as the ratio of data or packets at the source to the data or packets received at the destination .When the packet delivery ratio is 100% the network is more reliable. Thus we can say the packet delivery ratio must be as high as possible in order to improve the performance of the network.

End to End Delay (e2e): The time taken by a packet to be transmitted across a network from source to destination is termed as end to end delay. The end to end delay should be as minimum as possible in order to ensure reliable network

3. Proposed Work

According to the need and problem definition, proposed strategy should detect network vulnerabilities in the network. Several techniques have been proposed in order to prevent and detect gray hole attack .Patcha et al [8] proposed a method for the Gray hole attack prevention named as the watchdog method in which the nodes in the network are classified as trusted, watchdog and normal nodes. The watchdog node should observe its normal behavior node in order to decide whether they can be treated as trusted or malicious.

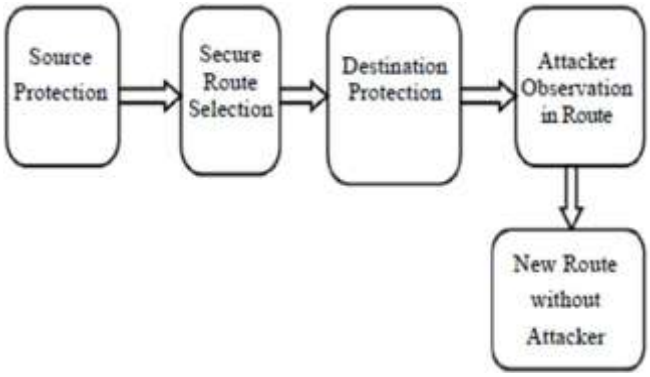

Figure 3.1: Overview of the proposed work

3.1 Watchdogs Mechanism

It is one of the intrusion detection techniques which detects the misbehaving nodes in the network[7]. In the figure shown below node D wants to send a message to node F which is not in its radio range . Due to this it sends the message through an intermediate node E. This node E after receiving the packet from node D forwards it to the node F. Let Sd be a set of nodes which hear messages sent from D to E and Sd be a set of nodes that hear message from E to F. This defines possible set of watchdogs of the node E as an intersection of Sd and Se. When a message is broadcasted in a network the packet is not only received by the intended node but it is also received by the neighbouring nodes. The watchdog method is a strategy proposed before in other studies that detects misbehaving nodes acting alone by maintaining a buffer that contains recently sent packets. When a node forwards a packet, the node's watchdog ensures that the next node in the path also forwards the packet.

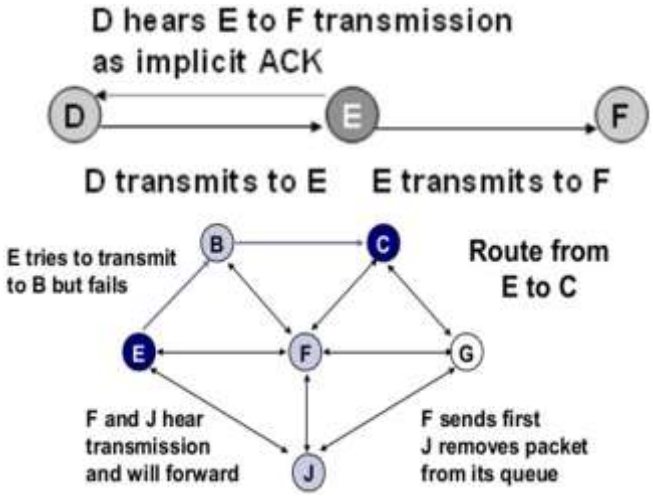

Figure 3.1: Watchdog Mechanism

4. Experimental Results and Analysis

4.1 Implementation of AODV Routing Protocol

The implementation of the protocol is carried out according to the metrics like packet delivery ratio and end to end delay. During the implementation procedure different nodes

are selected and for every selected node the packet delivery ratio is calculated. For example the node 10 has the packet delivery ratio as 81.88 and for node 20 it is 98.88 and so on.

Table 4.1 AODV Implementation with nn and PDR value

Nodes (nn)	10	20	30	40	50
PDR	81.88	98.88	98.88	98.75	98.93

From table we can see that the packet delivery ratio is different for all the nodes. The PDR should be 100% in order to make the network reliable.

4.2 Implementation of Gray Hole Attack in Ad hoc network using simulator

In this implementation there is an impact on the performance of network. The systems performance is degraded due to the loss of packets and this is due to the attack on the network. The malicious node drops the packet with a certain probability. If we compare the table 4.1 and 4.3 we will observe that the normal implementation of AODV for the 10 th node has the PDR as 81.88 but after the gray hole attack the PDR drops to 78.33 which ensures tht there is a loss of the packet. Similarly for the node 20 the PDR is 98.88 but after the gray hole attack the PDR drops to 88.17.And this goes for other nodes as well in which the PDR becomes less due to the gray hole attack.

Table 4.2: Gray Hole Implementation

Nodes(nn)	10	20	30	40	50
Gray hole	78.33	88.17	90.77	97.29	87.4

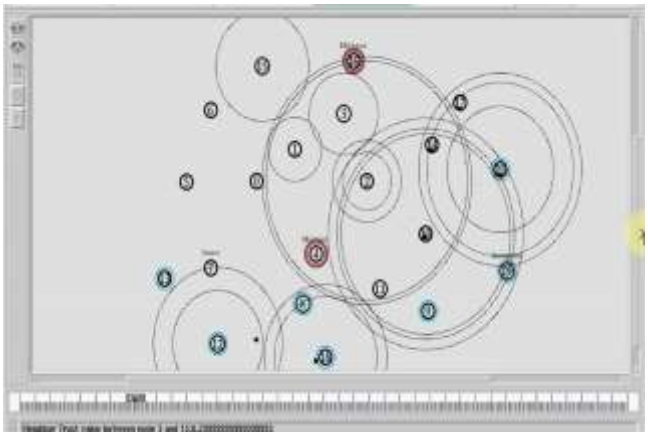

Figure 4.3: Gray Hole node on the AODV protocol indicated by red circle

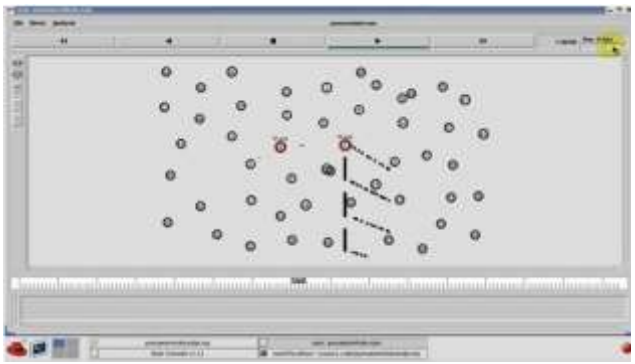

Figure 4.4: Gray Hole attack with different nodes in the network

5. Conclusion and Future Work

For any network performance is the main criteria . But due to the gray hole attack the performance of the network gets degraded .In this paper we have done the implementation of AODV protocol with PDR and e2e term and with their values the impact of gray hole attack has been analysed. Simulation of AODV as well as gray hole attack is carried out using ns-2 tool. To show the usefulness and results of the proposed approach implementation work on Network Simulator 2 tool is still in progress phase. Some of the future works includes method to secure the adhoc network, improve the performance of the network in order to ensure a reliable network.

References

[1] http://en.wikipedia.org/wiki/Personal_area_netwo rk, 25 July 2005.
[2] T. Franklin, “Wireless Local Area Networks”, Technical. http://www.jisc.ac.uk/uploaded_documents/WirelessL ANTechRep.pdf. 25 July 2005
[3] J. Reynold, “Going Wi-Fi”, Chapter 6, The Wi-Fi Standards Spelled out, Pg. 77.
[4] P. Misra,. “Routing Protocols for Ad Hoc Mobile Wireless Networks”, http://www.cse.wustl.edu/~jain/cis788-99/adhoc_routing/index.html, 14 May 2006
[5] P. Yau and C. J. Mitchell, “Security Vulnerabilities in Adhoc Network”.
[6] G. Vigna, S. Gwalaniand K. Srinivasan, “An Intrusion Detection Tool for AODV-Based Ad hoc Wireless Networks”, Proc. of the 20th Annual Computer Security Applications Conference (ACSAC’04).
[7] P. Ning and K. Sun, “How to Misuse AODV: A Case Study of Insider Attacks Against Mobile Ad-Hoc Routing Protocols”, Proc.of the 2003 IEEE Workshop on Information Assurance United States Military Academy, West Point, NY., June 2003