Study of various Attacks and Impact of Gray hole attack over Ad-Hoc On demand (AODV) Routing Protocol in MANETS

Aman deep Kaur, Prakash Rao Ragiri
Department of computer science and engineering,
Ambedkar Institute of Advanced communication technologies & Research,
Delhi

Abstract: Mobile Ad-hoc Network are dynamic networks, these networks Security of the Mobile Ad-hoc network is of great concern as the demand for reliability is getting important. Like other networks MANETS are prone to various attacks. One of routing misbehavior attack Gray hole attack targets the routing protocol of the network. Depending upon the nature of attack . This attack changes the performance of the network. Ad-hoc On-Demand Distance Vector (AODV) is prone to gray hole attack due to lack of central control and security. In this paper we are simulated the AODV protocol in different scenarios, the impact of gray hole attack in observed.

Keywords : MANET, Random Way Point, Manhatten grid , Routing misbehavior, Gray Hole Attack.

I. INTRODUCTION

Mobile Ad-Hoc Networks(MANETS) are networks which are created on demand, here each machine can perform the task of routing as well as accepting the data. These networks works on the basis of co-operation, here communication is done in either within the single hop or multi hop fashion, the trust among the node's are maintained so that they nodes can help the other node for data transmission. Providing flexibilty to network is one the benefits of Manets, but issues like security, limited resources cannot neglected. These days security, reliability are important concerns of any communication.

This paper focus on study of various attacks possible over Manets and analysis the impact of gray hole attack in different simulation models using Ns2.35 tool.

II. RELATED WORK

In [1] The author presented the various attacks like the Flooding attack, Impersonation attack, Worm hole attack, Black hole attack, Node isolation, sleep deprivation attack, the author also mentioned some solution to prevent such attack.

In[2] the author published various attacks and they are categorized into the following categories depending upon how they mislead the network: Modification, Interception, Fabrication and Interruption

In [3] the author presented the case study of insider attack and implemented over aodv, here author implemented the routing layer attack over AODV using Ns2.

In[4] the author surveyed Black hole attack over Manets. Described how the black hole impacts the network, types of Black hole ie single Black hole and the collaborative black hole.

In[5] the author implemented the gray hole attack in random way point model and analyzed the result by having 1,2,3,4 gray nodes in running scenarios. The network performance was analyzed Packet delivery ratio, Network routing load, total Drop packet ratio was observed. Under all the above performance metrics. The scenario with the 4 gray holes is recorder to have higher network routing load, packet drop ratio with packet delivery fraction.

In[6] author illustrated two main phases of gray hole attack and various other attacks that are possible in Manets like routing attack, worm hole attack.

In[7] the author describes the various attacks over manets and counter measure to wormhole and black , gray hole attack. The author proposed a countermeasure in which he used the table approach to mark the malicious node , To detect black and gray hole nodes, the sender occasionally check through all available routes to establish if the destination received all of its messages intact. This must be done after some data has been sent. In order to avoid any black hole nodes that might interfere with message traffic, the sender broadcasts a "check" request message and the destination's response would follow the same route as the request. To minimize the possibility of a node altering or faking the client's response, the sender compares each response with the data that it sent to the destination. If the responses differ from what the sender sent, it may indicate a bad link or a malicious node. If any two client responses vary, that is almost a sure sign of a malicious node .

In [8] The author implemented grayhole attack in free way mode and proposed a mitigation algorithm to overcome such attack later compared the result on the basis of Throughput, Packet delivery ratio, Network routing load and End to End delay.

In[9] the author implemented an algorithm in which provides the detection mechanism, here trust and cooperation both the properties are used to locate the gray hole , here for different modules are initiated one after the other in order to alarm the gray hole nodes , not only detection of gray hole is important ,but also reducing the no. false positives is also important.

III. AODV

Manets comprise of various routing protocol , these can be proactive , reactive and Hybrid , depending upon the nature that how the nodes send routing information to each other , Ad-hoc On demand distance vector protocol is one of the reactive protocol of manets, which is used to establish the connection. This protocol come into picture when nodes wants to communicate with each other but does not finds the route to forward the packet. As we know that the nodes can easily transmit the packet to the nodes which comes under same frequency range. Whenever nodes are not in same transmission range they need to depend on the co-operation of other nodes to transmit the data.

The aodv uses route establish mechanisms , route maintenance mechanisms .It uses four different messages to do all the above process, hello, rreq, rrep, rrer. Initially all the nodes broadcast the hello messages, to detect the neighbor. It will send rreq message to the neighbor nodes which contains the sequence no. of the destination, source address, destination address. This process is carried till the node finds the destination with higher sequence no. Once the node finds the route it will send rrep message which contains the next hop address. Rerr message is used for error in route , when node sense the error it will pass the rerr message in order to re-establish the route.

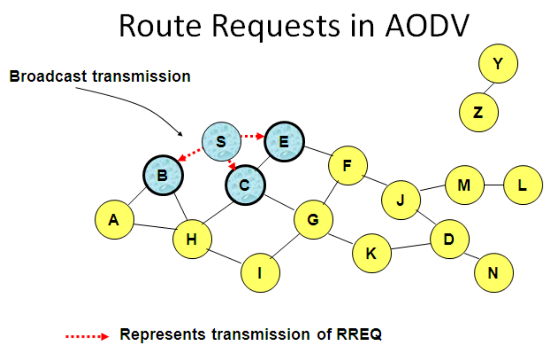


Fig 1: Route Request in AODV

Since Aodv provides no mechanism for security, it is easy for attacker to attack such weak routing. Most of the attacks are done by insider attack, one such attack is gray hole attack, which is also called as selective droping attack. This attack take the benefits of the cooperativeness of nodes in order to make the connection.

IV. GRAY HOLE ATTACK

In this kind of attack the attacker misleads the network by approving to forward the packets in the network. As soon as it receive the packets from the neighboring node, the attacker falls the packets, This attack comes under the category of active attack. In the beginning the attacker nodes behaves usually and reply true RREP messages to the nodes that started RREQ messages. When it receives the packets it starts dropping the packets and launch Denial of Service (DoS) attack. The malicious activities of gray hole attack may be different from time to time . It may 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. Due this behavior it is very tricky for the network to figure out such kind of attack. Gray hole attack is also termed as node misbehaving attack.

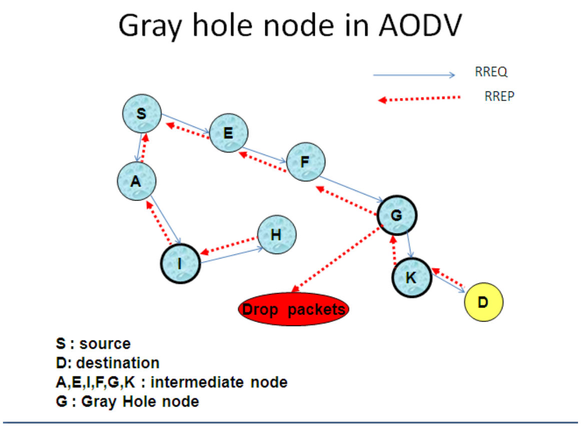


Fig:2 Gray hole nodes in AODV

V. MOBILITY MODEL

In Manet s the mobility models the way in which nodes might move in a real world environment. A mobility model is designed to represent the movement patterns, their location at a particular instance of time, direction of movement, pause pattern, and speed changes over time of the mobile nodes in a given scenario. There are various Mobility models suited for Manets, depending upon the requirement two such models are discussed here:

Random Point Model

This model works on the principle that the nodes are free to move anywhere in any direction, The nodes may pause upto certain desired time .In this model a certain area is to be allocated like 750*750 m in which nodes may move the duration of the simulation ,the send rate has to be specified.

ManhattenGrid Model

This is Model is also used Manet, in this the nodes are bounded to move either straight ,left or right with some probability. This model is stricter than RandomWay Point and nodes are bounded to move in lanes only and can take specified direction. In this we need to specify the maximum nodes, minimum speed, and lanes in manhatten grid fashion. Bonnmotion tool is used to create both of the above mentioned scenarios.

VI. SIMULATION AND RESULTS

To create the above mentioned models,a tool called bonnmotion is used. Both of the scenarios can be easily constructed by providing the details like duration, speed , x coordinates and y coordinates, pause time etc. Connection are established using tool cbrgen.tcl which is available in ns2.35 package .

Simulation Metric

Parameter	Values
No.of Nodes	10 to 50
Simulation Area	750*750
Simulation Time	600 sec
Mobilty Model	Random Way point , Manhatten grid
Traffic /connection	Cbr over UDP
Mac	802.11
Protocol	AODV

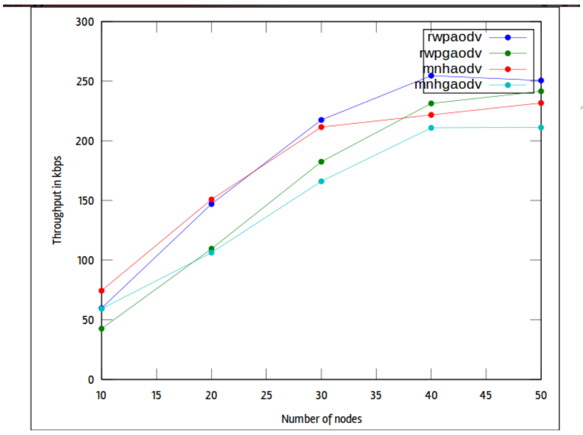
Table 1: simulation Metrics

In this work we used ns2.35 tool for the purpose of simulation, in this without any modification we have implemented AODV and later recompiled ns2.35 with the changes of gray hole attack. In gray hole implementation we have taken 10% of the nodes are gray hole nodes. Simulation metrics are the inputs and outputs are observed in terms of Average Throughput, Packet delivery ratio ,Packet drop Ratio.

Average throughput

It describes the actual data rate of the network. High throughput is desired for the networks, It is defined by mathematical formula:

Avg throughput =total data sent (kb)/total time (s)



In fig 3:Avg Throughput

In fig 3 it is clear that throughput of network having gray holes nodes is less as compared to normal AODV routing protocol in both random way point and manhatten grid scenario.

Packet delivery ratio

Packet delivery ration defines the network efficiency hence one of the important parameter , for better performance it is desired to have high packet delivery ratio, it signifies the efficiency of routing protocols.

Packet delivery ratio= total no . packets received /total no. of packets send.

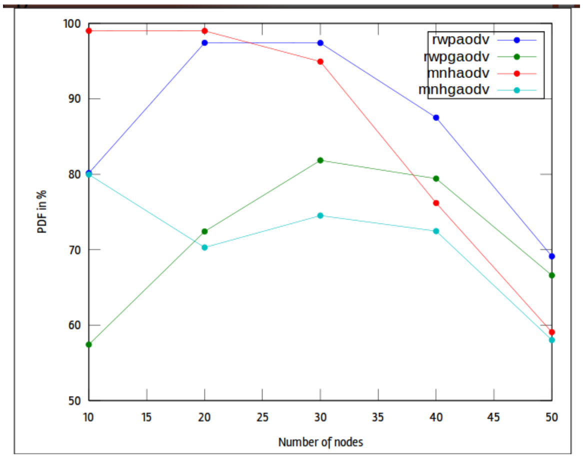


Fig 4:Packet Delivery Ratio

The fig4 clearly show impact of gray hole attack over AODV by having lower pdf as compared to Aodv routing protocol .

Fig 4 Packet delivery Ratio

Packet drop ratio

It is defined as total number of packets dropped during simulation For the better performance of a network this ratio should be minimum.

P drop ratio = No.send packet- No. Received packet.

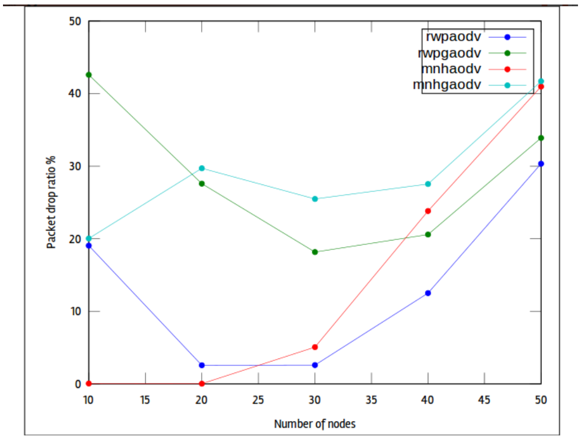


Fig 5 :Packet Drop Ratio

VI CONCLUSION

Using Ns2.35 impact of the gray hole attack is observed over AODV, by varying Number of nodes and misbehaving nodes for different scenarios. The comparisons is done on the basis of average throughput, Packet delivery ratio, packet drop ratio. We found that by having gray hole nodes in the network the performance of the network is degraded in Manets.

VII REFERENCES

1. Sudhir Agrawal, Sanjeev Jain, Sanjeev Sharma," A Survey of Routing Attacks and Security Measures in Mobile Ad-Hoc Networks", JOURNAL OF COMPUTING, VOLUME 3, ISSUE 1, JANUARY 2011, ISSN 2151-9617
2. S. A. Razak, S. M. Furnell, P. J. Brooke," Attacks against Mobile Ad Hoc Networks Routing Protocols"
3. Peng Ning *, Kun Sun," How to misuse AODV: a case study of insider attacks Against mobile ad-hoc routing protocols", Elsevier Journal Adhoc Network 3 (2005)795-819
4. Fan-Hsun Tseng1, Li-Der Chou1 and Han-Chieh Chao," A survey of black hole attacks in wireless mobile ad hoc networks," Human-centric Computing and Information Sciences 2011
5. G.Usha and Dr. Bose, "Impact of Gray Hole Attack on Ad-hoc Networks "
6. V.SHANMUGANATHAN, Mr.T.ANAND M.E," A Survey on Gray Hole Attack in MANET",IRACST – International Journal of Computer Networks and Wireless Communications (IJCNWC), ISSN: 2250-3501 Vol.2, No6, December 2012
7. B.Revathi, D.Geetha," A Survey of Cooperative Black and Gray hole Attack in MANET ",International Journal of Computer Science and Management Research Vol 1 Issue 2 September 2012
8. Ashish Joshi, Ram Shringar Raw, Prakash Rao Ragiri , "A Counter Based Approach for Mitigation of Grayhole Attack in VANETs: Comparison and Analysis ", International Journal of Scientific and Research Publications, Volume 3, Issue 6, June 2013
9. Jaydip Sen, M. Girish Chandra, Harihara S.G., Harish Reddy, P. Balamuralidhar," A Mechanism for Detection of Gray Hole Attack in Mobile Ad Hoc Networks", ICICS 2007