Detecting and Defending Black Hole Attack in MANET using AODV

[1]B.Jayasree, [2]B.Chandra mouli
[1]PG Student, [2]Asst.Proffessor
[1,2]Department of CSE
[1,2]Siddharth institute of Engineering & Technology, Puttur, India

Abstract: Wireless mobile ad hoc network (MANET) is vulnerable to various attacks due to lack of infrastructures. With the attacks they make the information not useful for the users. In MANETS routing is one the special component and it has several routing protocols, which are affected by various attacks. Black hole attack is one of the well-known security attacks in wireless ad hoc network. Many researchers have proposed different techniques of AODV protocol to detect and protect from black hole attacks. This paper discusses the detection and prevention of black hole attack on MANET using the trace file analysis obtained using the Network Simulator.

Keywords: Black Hole Attack, AODV (Adhoc On-Demand Distance Vector Routing Protocol), MANET (Mobile ad-hoc Network), Network Simulator 2.

1. Introduction

Mobile Ad Hoc Network (MANET) is the independent arrangement of mobile nodes connected to each other by wireless linkages. Each node operates as an individual system as well as a router to advance packets further. The nodes are free to move around and establish themselves into a network. The link between each pair of the nodes may be more than one. This will allow an association of various links to be a part of the same network. These networks do not require any permanent arrangement of base stations. This feature allows the connection of all the mobile devices fast and spontaneously. It is a peer-to-peer mode of operation that can significantly lengthen the distance of the wireless networks.

Wireless networks are prone to various security attacks. A black hole attack is a type of attack that seriously affects data collection in WSN. When black-hole node receives this request it immediately sends a reply to the broadcaster claiming that it has the freshest and the shortest path to the destination node. Source node believes that reply because there is no mechanism to verify that the request is from a normal node or from a black-hole node. Source node starts forwarding packets to black-hole node hoping to deliver these packets to the destination node, then black-hole node starts to drop these forwarded packets To overcome this problem, an detection based security and prevention is proposed to find out the shortest path using secure communication by analysing the trace file. Detection and prevention can significantly improve the data route success probability and ability against black hole attacks and also optimize network lifetime.

2. Related Work

Ioannis Broustis Gentian Jakllari Thomas Repantis Mart Molle[1] discuss the performance of routing protocols for large scale mobile ad hoc network larger throughput lower end to end delay fewer lost data packet. They perform the simulation on DSR, TORA, AODV, LAR in the paper discuss result derived from extended simulation and compare the efficiency of the above four protocols using NS-2 and Qualnet.

Satoshi Kurosawa, Hidehisa Nakayama [2] has been analyzed the blackhole attack which is one of the possible attacks in ad hoc networks. In a blackhole attack, a malicious node impersonates a destination node by sending a spoofed route reply packet to a source node that initiates a route discovery. By doing this, the malicious node can deprive the traffic from the source node. In order to prevent this kind of attack, it is crucial to detect the abnormality occurs during the attack. After analysis he proposed an anomaly detection scheme using dynamic training method in which the training data is updated at regular time intervals.

Md. Anisur Rahman, Md. Shohidul Islam [3] compared the performance of two prominent on-demand reactive routing protocols for mobile ad hoc networks: DSR and AODV, along with the traditional proactive DSDV protocol. A simulation model with MAC and physical layer models have been used to study interlayer interactions and their performance implications. The On-demand protocols, AODV and DSR perform better than the table-driven DSDV protocol.

Arathy K Sa, Sminesh C Na [4] suggest the black hole detection schemes, which detect both single and collaborative attacks. They proposed D-MBH algorithm to detect single and multiple black hole nodes with the use of an additional route request with nonexistent target address, computes a threshold ADSN, creates a black hole list and invokes the proposed D-CBH algorithm. With ADSN, black hole list and next hop information extracted from RREP, then a list is made by D-CBH algorithm of collaborative black hole nodes. This algorithm reduced routing and computational overhead.

SiddharthDhama, Sandeep Sharma, MukulSaininormal [5] purposes the model in five cases with each one having 20 nodes where the protocol used is AODV, than after that the same is tested with BH node. Then again simulated 20 node model with solution that resulted in decreasing the effect of BH node. AODV operation has minimum packet loss but when a BH node is introduced in the network the packet 556 Nancy Mittal and Lal Chand loss has increases to 88%. When we used the IDSAODV in the same network packet loss are decreased to 66%. 7.

NidhiChoudhary, Dr.LokeshTharani, [6] proposes a timer based detection approach for identifying black hole node. In network layer they proposed a Timer based method to overhear the next node action. As black hole attack causes great damage to the network performance, and it degrades further with the increase in the number of attackers in the network. Once this is the case the attack is done on the active flows by the attackers which results in packet drops, proposed method can be adopted.

Pramod Kumar Singh, Govind Sharma [7] proposed with uses promiscuous mode of the node. This mode allows a node to intercept and read each network packet that arrives in its entirety, in other words, promiscuous mode means that if a node A within the range of node B, it can overhear communication to and from B even if those communication do not directly involve A. It does not require any database, extra memory and more processing power

Sagar R Deshmukh, P N Chatur, Nikhil B Bhople [8] proposes an AODV based secure routing mechanism to detect and eliminate black hole attack and affected routes in the early phase of route discovery. A validity value is attached with RREP which ensures that there is no attack along the path. This validity value is attached with the RREP message and is stored in route table at each node of active path. Whenever a node receives route request, if it is the intended destination or possess a legitimate route, then route reply message will be generated by setting value for validity bit in RREP (Here legitimate route refers to the route for which validity bit in route table is set). This RREP then will be sent back to its neighboring hop from which it obtained RREQ. The proposed route reply message differs in the validity value with the fundamental AODV route reply message. Proposed system neither requires heavy processing nor extra memory. With the addition of negligible overhead, black hole attack is prevented before actual data transmission phase.

3. AODV (Adhoc On-Demand Distance Routing Protocol)

In MANET AODV routing protocol is an on-demand routing protocol used to finding a route to the destination. All mobile nodes work cooperatively to finding route to the destination using the control messages of routing protocol. In AODV routing protocol routes are maintained just as long as it is needed. AODV routing protocol uses the destination sequence number for each route entry, which is a distinguishable feature from other routing protocol. In AODV routing protocol the routing table stores the destination address, next-hop address, destination sequence number and lifetime. In this, when a node wishes to send a packet to some destination, it checks its routing table to determine if it has a pre-established route to the destination. If it has a pre-established route to the destination, it forwards the packet to next node. If it has not a pre-established route to the destination it launches a route discovery process. For establishing a route to the destination the AODV protocol use the Route Requests (RREQs), Route Replay (RREPs), Route Errors (RERRs) control messages. The source node broadcasts an RREQ message when it wants to established a communication with the targeted node. This RREQ message is inseminated from the source and received by intermediate nodes (neighbours of the source node). When RREQ is received by a transitional node, it fast checks its routing table to find a fresh route towards the destination that is requested in RREQ. A route reply (RREP) message is sent towards the source node through the re-established reverse route (established when RREQ pass through intermediate nodes) if such a route is found. If the transitional node cannot able to find a route, it restores its routing table and sends RREQ to its neighbours. This action is repeated until the destination nodes receive the RREQ of source node.

4. Black Hole Attack

MANETs are vulnerable to many security attacks, where one of these attacks is the black hole attack. Black hole attack is an attack that disrupts the route between the victim nodes to a given destination, or invades the route in between, by suppressing other alternative route. In a black hole attack, where the malicious node advertises itself that it has the shortest route to the destination and tries to fool the source node. After the response received from the malicious node, the source node leaves all other paths and transferring data to the malicious node. Instead of forwarding to the next node, a malicious node leaves all data packets

after data packets are received from the source node. Common two classifications of black hole attacks are listed as: (i) Single Black Hole (SBH), and (ii) Cooperative Black Hole (CBH). In SBH attack, only one malicious node is present and whereas in CBH attack, there is two or more malicious node attack in cooperation with each other.

5. Proposed Work &Methodology

In this paper an implementation of black hole in wireless adhoc network is implemented using ns2.35 through AODV and the trace file analysis is performed using awk. The performance is measured based on different parameters extracted from the trace file like Packet delivery ratio, Packet drop ratio, etc.

The black hole attack in the network is detected based on the packet drop values observed at each node using a threshold value and performance is analysed (with and without black hole attack). X-Graphs are generated and observed to see how the number of packets dropped changes before, during and after the black hole attack. All simulations have been performed using NS2.35 simulator.

6. Simulation Environment

In this paper work all the simulation work is performed in network simulator version 2.35. All the simulation work was carried out using TCP/UDP variants with AODV routing protocol. Network traffic is analysed by using the trace/log file. Wireless network which we have used has been simulated using simulator and trace files obtained are analysed using the awk.

7. Detection Technique

The proposed work describes the detection of black hole attack in MANET. The system is based on analysis of trace file obtained during the simulation of black hole attack in ns2.35. The trace file analysis is done using different parameters such as packet delivery ratio, packet drop ratio, etc. The trace file analysis is performed to identify the critical nodes as well as the safe nodes. On each node, the trace analysis is done to identify the nodes which are dropping the packets beyond a threshold value. The process is repeated on each node until we classify the nodes as safe and malicious nodes. Once the nodes are marked as malicious, they are removed from the network. The system with black hole attack has less throughput value and high packet loss over the network. Once the malicious nodes are removed from the network, new routing tables are created using the AODV protocol. This enhances the throughput and reduces the packet loss ratio. The system is implemented in a wireless adhoc network using AODV protocol.

8. Prevention Technique

Once the black hole nodes are detected, the nodes are then removed from the network by classifying them as malicious nodes. New and secure routing is established using the safe nodes that are remaining in the network using the AODV protocol. These new routing tables are used to establish communication among the remaining safe nodes. The process is repeated until the network is free from black hole nodes and proper communication is established among the nodes. This ensures high throughput and less packet loss which is desired and hence, enhances the security and trust in the network.

9. Results

The simulation is done using NS2 and following results are produced when AODV protocol is implemented. Following figure shows the simulation of black hole attack using the Network Simulator 2.

Network without Black Hole Attack in ns2

The simulation is done to create 6 nodes. Communication between the nodes in the network without black hole attack using AODV protocol is shown. Packets are sent from Source(Node0) to Destination(Node5) via intermediate nodes(Node1 and Node3).

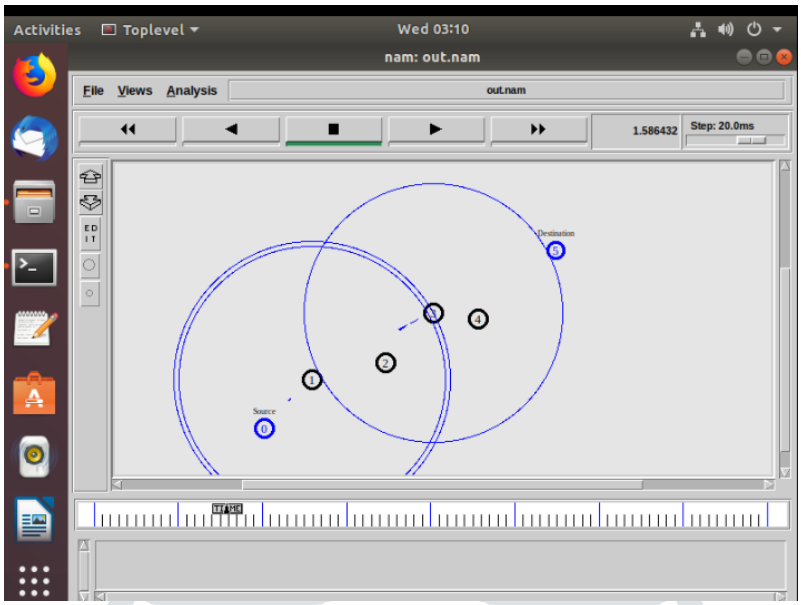

Fig 1: Network without black hole attack in ns2

Network with Black Hole Attack in ns2

The simulation of network with Black Hole Attack is done, where malicious nodes are entered into the given network which act as normal nodes but are malicious and damages the secure communication.

After Black hole attack is simulated data flows from the source node(Node0) to the Attacker node(Node1).

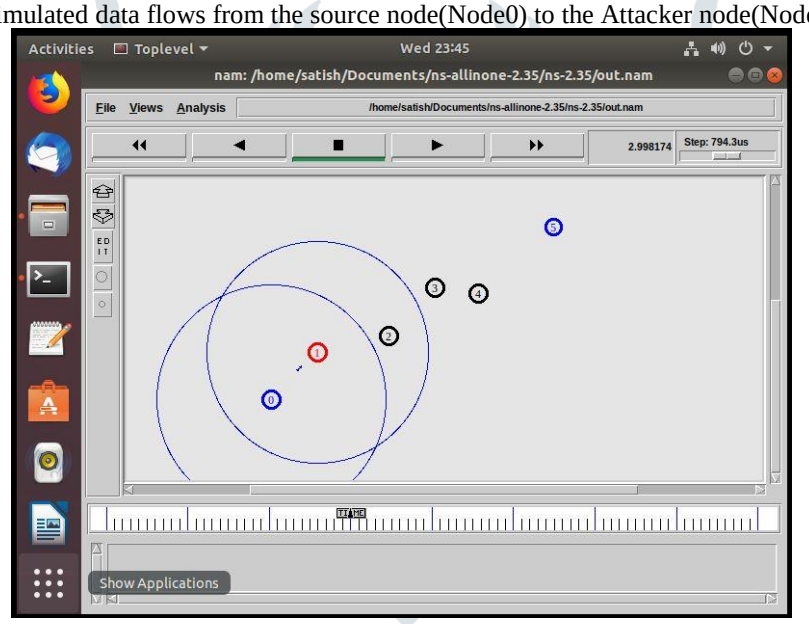

Fig 2: Network with one Black Hole Attack

After preventing black-hole attacks in ns2

The simulation of AODV routing protocol after preventing black hole attacks is shown. After using detection technique, nodes 1 and 3 are detected as malicious nodes. The malicious nodes detected are removed from the network. New routing tables are then computed using the AODV protocol. The data then flows from source node (Node0) to destination node (Node5) via node 2 and node 4.

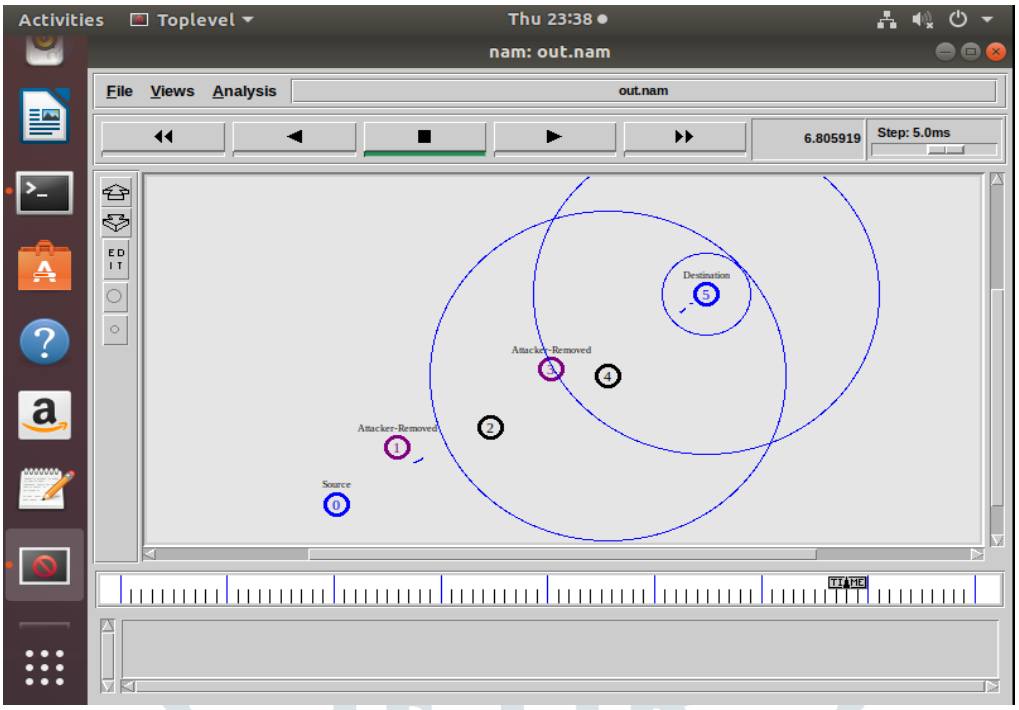

Fig 3: After removing the black hole nodes from the network in ns2

Detection of black hole attack:

```
num_nodes is set 6
INITIALIZE THE LIST xListHead
using backward compatible Agent/CBR; use Application/Traffic/CBR instead
Start of simulation..
channel.cc:sendUp - Calc highestAntennaZ_ and distCST_
highestAntennaZ_ = 1.5,  distCST_ = 550.0
SORTING LISTS ...DONE!

Blackhole Nodes :
Node Packets_Dropped
   1              34
   3              25

Before first black hole attack :

packets_sent:49
packets_received:49
Packet Delivery Ratio:100.0000 %

During first black hole attack :

packets_sent:33
packets_received:1
Packet Delivery Ratio:3.0303 %

After preventing first black hole attack :

packets_sent:75
packets_received:72
Packet Delivery Ratio:96.0000 %

During second black hole attack :

packets_sent:25
packets_received:1
Packet Delivery Ratio:4.0000 %

After preventing second black hole attack :

packets_sent:66
packets_received:62
Packet Delivery Ratio:93.9394 %
```

Fig 4: Detection of Black Hole Attack

Performance analysis before, during and after the black hole attack:

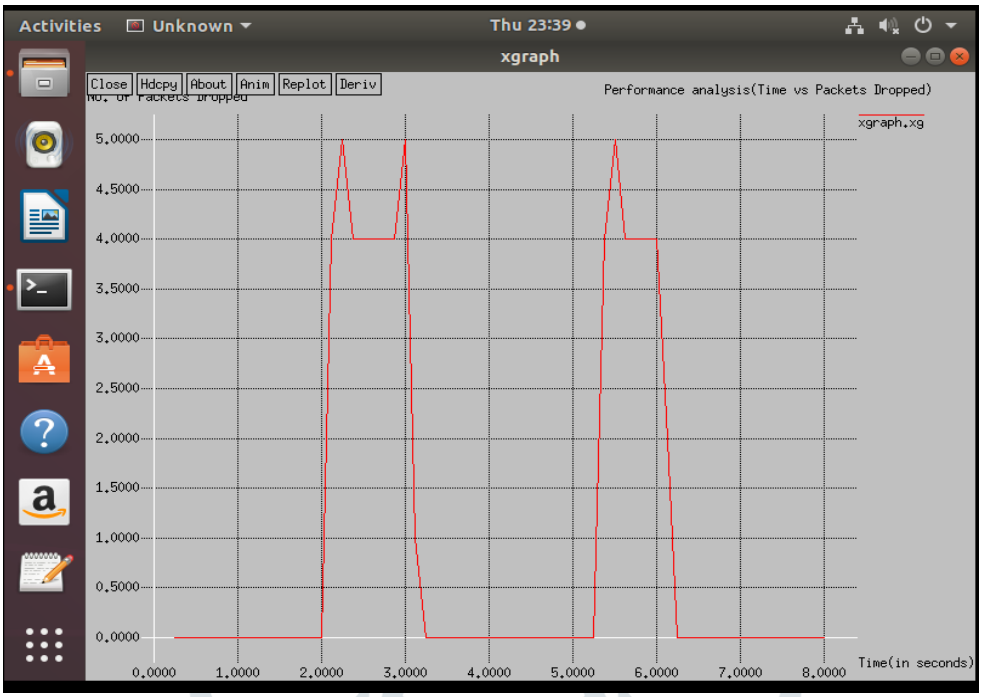

Fig 5: Performance analysis before, during and after the black hole attack (Time vs Packets Dropped)

10. Conclusion

Black hole attack is one of the most important security problems in MANET. The proposed work analyses the effect (number of packets dropped) during the black hole attacks on MANET. The nodes are classified as safe and malicious, using the data obtained from trace/log file. The malicious nodes are then removed from the network and secure communication among the other nodes is created using the AODV protocol.

11. Future Work

In this paper we have reviewed the AODV protocol and Black hole attack in MANETs. We have discussed feasible solutions that can be implemented to detect and prevent the black hole attacks using the trace file analysis. The proposed method can be used to find the secure routes and prevent the black hole nodes in the MANET. The work mainly focuses on black hole attack but can handle also other misbehaviour patterns like dropping packets and so on. It can be improved in order to handle the packets (like considering only data packets when control packets are forwarded as well). Additional mechanisms to work in the field of QoS (quality of service) and to increase the fairness in the network are possible areas for future research. As future work, we intend to develop simulations to analyse the performance of the proposed solution based on various security parameters like throughput, mean delay time, packet overhead, memory usage, mobility, increasing number of malicious nodes, increasing number of nodes and scope of the black hole nodes.

12. References

[1]Nancy Mittal," Prevention and Detection Techniques under Black Hole Attack in MANETS: A Survey"**,** ISSN 0973-6972 Volume 10, Number 4 (2017), pp. 551-558M.Tech Student, Department of Computer Engineering, Punjabi University, Patiala, Punjab, India.

[2] **Ashok Koujalagi,"**Considerable Detection of Black Hole Attack and Analyzing its Performance on AODV Routing Protocol in MANET (Mobile Ad Hoc Network)"**.** June 22, 2018,Department of Computer Science, Basaveshwar Science College, Bagalkot, Karnataka, India.

[3]Swati Saini1 ,VinodSaroha, "Analysis and Detection of Black Hole Attack in MANET",India Online ISSN: 2319-7064 BPSMV University, School of Engineering and Science Kanpur, Sonipat, India.

[4] Monika Roopak, Bvr Reddy, "Blackhole Attack Implementation In AODV Routing Protocol", International Journal of Scientific & Engineering Research, Volume 4, Issue 5, May-2013.

[5] Mohamed Elboukhari, MostafaAzizi and AbdelmalekAzizi, "Impact Analysis of Black Hole Attacks On Mobile Ad Hoc Networks Performance" , International Journal of Grid Computing & Applications (IJGCA) Vol.6, No.1/2, June 2015.

[6]Virendra Singh Kushwah "Implementation of NewRouting Protocol for NodeSecurity in a Mobile Ad Hoc Network" (IJCSIS) International Journal of Computer Science and Information Security,Vol. 8, No. 9, December 2010.