Blackhole Attack in MANET - NS2 Analysis

Prasad Ghatol[1], P. G. Chilveri[2], Onkar Gharapurkar[3], Shubham Domale[4]

[1,2,3,4] *Dept. of E & TC Engg., Smt. Kashibai Navale College of Engineering, Savitribai Phule Pune University, Pune*

[1]*prasadnghatol@gmail.com*

[2]*pgchilveri@gmail.com*

[3]*omgonkar@gmail.com*

[4]*domaleshubham95@gmail.com*

Abstract

Mobile Ad hoc Network (MANET) is a type of wireless networks that provides numerous applications in many different areas. An ad-hoc network is an infrastructure less network, which is a collection of mobile nodes, which are arranged in a dynamic form. This network is an independent and isolated network. Security of MANET had become one of the important topics in networks fields. MANET is prone to different types of attacks,which affect its functionality and connectivity. The black-hole attack is considered one of the most widespread active attacks that degrade the performance and reliability of the network. This is dueto themalicious node, which drops all the packets received by it.

Keywords- *Black Hole Attack, NS2, MANET, Black Hole Detection, Black Hole Prevention.*

I. INTRODUCTION

A mobile ad hoc network (MANET) is relatively new in mobile communication. MANET has received spectacular consideration because of the self-configuration and self-maintenance property of MANETs. A MANET is a network, which consists of several mobile nodes, which are connected to each other by wireless links. Each mobile node can act as a host and also as a router, to establish a route. When a source node intends to send the data packets to the destination node, then the packets get transferred through the intermediate nodes present in the network. Thus, for this purpose, quick deployment of the nodes is needed, in order to establish a route, and this is an important issue in MANET.

Black hole attack is a special type of attack, in the Reactive protocols. A black-hole node, is a malicious node in the network that attracts the packets by falsely claiming, that either it has shortest route to reach the destination or it is the destination itself, and then, it drops the packets.

These Black hole nodes may can have various harmful actions on the network, such as:

i) It can behaves as a Source node by falsifying the Route Request packet.
ii) It can behaves as a Destination node by falsifying the Route Reply packet.
iii) It can decrease the number of hop count, when forwarding Route Request packet.

II. LITERATURE SURVEY

Sr. No.	Reference	Purpose	Merits	Demerits
1]	Prevention of Black Hole Attack on MANET Using Trust Based Algorithm (Apurva Jain, AnshulShrotriya)	Classification of Attacks. To implement Trust Based Algorithm, for Prevention of Black Hole Attack.	Throughput increases and Energy decreases	Higher end-to-end Delay
2]	Black Hole along with Other Attacks in MANETs: A Survey (Fan-Hsun Tseng, Hua-Pei Chiang, Han-Chieh Chao)	Information regarding Routing Protocols, to Detect and Prevent Non-Cooperative Black Hole Attack.	A number of open issues are listed	Techniques not much used
3]	Prevention and Detection Techniques under Black Hole Attack in MANETS: A Survey (Nancy Mittal, Lal Chand)	Information regarding Black Hole Attacks.	Effects of Black Hole Attacks can be reduced, by implementing different techniques	Algorithm not much effective
4]	A Literature Survey of Black hole Attack in MANET (Monika Shivhare, Prof. Praveen Kumar Gautam)	Information regarding Attacks in MANETs.	Higher packet delivery ratio	Due to the unspecified design there are many limitations of routing protocol in MANETs
5]	Detection and Prevention of Black-Hole Attack in MANETS (Rashmi, AmeetaSeehra)	Information regarding Black Hole Attacks.	Higher Detection Rate (DR), Packet Delivery Ratio	Lower Throughput
6]	Detection and Prevention of Black Hole Attack in MANET (Veenita, Shamsher Singh Malik)	Information regarding Co-Operative Black Hole Attack.	The proposed solution can be applied to identify and remove any number of Black Hole or Gray Hole Nodes in a MANET	Delay is higher
7]	Prevention of black hole attack by different methods in MANET. (NakkaNandini, Reena Aggarwal)	Information regarding Single Black Hole Attack.	Black Hole attack are prevented in some extent in the networking environment	Lower Accurate Threshold value
8]	Different types of attacks in Mobile ADHOC Network: Prevention and mitigation techniques (Aniruddha Bhattacharyya ArnabBanerjee Dipayan	Information regarding different types of Attacks in MANETs.	Categorized different types of ad hoc security attacks solely based on their characteristics	More powerful algorithms required for DATA and CONTROL traffic attacks.

	Bose)			
9]	A survey of black hole attacks in wireless mobile ad hoc networks Fan-Hsun Tseng1, Li-Der Chou1 and Han-Chieh Chao2,3,4	Information regarding different Single Black Hole Attack Detection Schemes	Proactive detection method has the better packet delivery ratio and correct detection probability	Attackers are able to avoid the detection mechanism
10]	Detecting and Isolating Black-Hole Attacks in MANET Using Timer Based Baited Technique (AdwanYasin and Mahmoud Abu Zant)	Information regarding different Black Hole Attack Detection and Isolation Methods.	TBBT integrates both timers and baiting techniques in order to enhance black-hole detection	Lower Throughput, End-to-End Delay, and Packet Delivery Ratio.
11]	SURVEY OF BLACKHOLE ATTACKS ON AODV PROTOCOL IN MANET (Khushbu Patel)	Information regarding ADOV Routing, Black Hole Attack and its Solution.	A Comparison among the available methods for Black Hole Detection and Prevention.	More Time Delay, Network Overheads.
12]	Solution to Black Hole Attack in Ad Hoc on Demand Distance Vector Routing Protocol (Ahmed Ibrahim, Nagy E Zaki)	Information regarding Solution to Black Hole Attack in Ad Hoc.	Higher Security and have less Packet Drops.	Lower Throughput.
13]	BlackHole Attack and Detection Method for AODV Routing Protocol in MANETs (VipinKhandelwal, Dinesh Goyal)	Information regarding Detection and Prevention of Black Hole Attack in MANET.	This technique is useful for other routing protocols to isolate malicious nodes in the network.	Detection is difficult due to resources constraints.
14]	Identifying & Isolating Multiple Black Hole Attack on AODV protocol in MANET (AmanSaurabh, RakeshYadav, Harjeet Kaur)	Information regarding Identifying & Isolating Multiple Black Hole Attack in MANET.	The proposed Algorithm can work Effectively & Efficiently in both single & multiple Black Hole Attacks.	Cannot detect Collaborative Black Hole Attacks.
15]	Modified AODV Protocol for Detection and Prevention of Black hole Attack in Mobile Ad Hoc Network (NeelamJanak Kumar Patel, Dr. KhushbooTripathi)	Information regarding Modified AODV Protocol for Detection and Prevention of Black Hole Attack.	End to end delay is good.	Low Throughput & Packet Delivery Ratio.

III. AD-HOC NETWORKS

"Ad hoc" is a kind of makeshift, improvised network, hence a wireless ad hoc network (WANET) is a type of on-demand, impromptu device-to-device network. In ad hoc mode, a wireless connection can be set directly to another computer or device, without having to connect to a Wi-Fi access point or router. Due to the nature of ad hoc connection, which does not need an existing infrastructure, to sustain the network, it is entirely decentralized and is also considered as a peer-to-peer network. Ad hoc does not use a central managing device (like a router), where the network's data is constantly flowing, in and out of the network and nodes. Every single node in the ad hoc network, forwards data evenly throughout the entire structure.

Types of Ad-Hoc Networks are:

i) Mobile Ad Hoc Networks (MANETS).
ii) Vehicular Ad Hoc Networks (VANETS).
iii) Smartphone Ad Hoc Network (SPAN).
iv) Wireless Mesh Network.
v) Army Tactical Manet.
vi) Wireless Sensor Network.
vii) Disaster Rescue Ad Hoc Network.

IV. MANET

MANET stands for Mobile ad hoc Network. MANET usually has a routable networking environment, which works on top of a Link Layer ad hoc network. MANET consist of multiple wirelessly connected mobile nodes. These nodes in the network are self-configuring, self-healing nature, and does not have a fixed infrastructure. MANET nodes freely move around the network, as the network topology changes frequently. Each node also behaves as a router, as a result they can forward traffic to other specified node in the network.

MANET can operate as either in standalone fashion or they can be a part of larger internet group. MANET form highly dynamic autonomous topology with the presence of one or multiple different transceivers between nodes.

Characteristics of MANETs are:

i) Dynamic Topologies.
ii) Bandwidth Constrained, Variable Capacity Links.
iii) Autonomous Behavior.
iv) Energy Constrained Operation.
v) Limited Security.
vi) Less Human Intervention.

V. MANET ROUTING PROTOCOLS

Routing is an important feature in any network, whether it may be for wired or for wireless. The protocols which are designed for routing in each of the two types of networks, namely wired networks and wireless networks, have totally different characteristics. Routing protocols for wired networks, does not need to handle mobility of nodes within the system, and neither do they have these protocols to be designed which will minimize these communication overhead. This is because generally wired networks have high bandwidths. Most importantly, the routing protocols in wire line networks or wireless infrastructure network are assumed to execute on trusted entities, namely the routers. But in case of MANETs, there are no special routers. Hence, each node present in the network has to perform routing functions in order to forward a packet to the destination. As a result mobility is a basic feature in MANET. Apart from this, resource constraints also govern the design of routing protocols for such networks. Therefore, these routing protocols need to be specifically designed for MANET.

The Types of MANET Routing Protocols are:

i) Proactive Routing Protocol.
ii) Reactive Routing Protocol.
iii) Hybrid Routing Protocol.

VI. ATTACKS IN MANETS

Due to lack of trusted centralized authority and limited resources, MANETs are more vulnerable to security attacks. In MANET, the nodes which are within the wireless transmission ranges of each other, they can communicate directly. However, the nodes which are outside the range of each other, they have to rely on some other intermediate nodes to relay the messages. Hence, any routing protocol which is used, needs to encapsulate an essential set of security mechanism. These mechanisms are useful for detecting, preventing and responding to any kind of attack on the network.

The major security goals that needs to be addressed for maintaining a reliable and secure ad-hoc network environment are:

i) Confidentiality.
ii) Availability.
iii) Authentication.
iv) Integrity.
v) Non-repudiation.

Types of Attacks in MANETs are:

i) External Attack.
ii) Internal Attack.
iii) Passive Attack.
iv) Active Attack.
v) Routing Attack.
vi) Resource Consumption Attack.
vii) Other Attacks.

VII. BLACKHOLE ATTACK IN MANET

Security of the network, is among the main research topics in the field of computer networks. One of the most famous attacks, in networks, is the Black Hole attack. A black hole attack is an attack where the malicious node forcibly obtains the route with greatest sequence number and less hop count and subsequently overhears or drops all data packets. The security of the network is important, due to the extensive use of ad hoc networks in the martial environment and other security sensitive fields. As the nodes participate in the routing process, it may be possible that, they can destroy the network. As the routing procedure is based on some kind of trust between nodes present in the network, it can provide a good chance for attackers to make an attack on the network, in order to disorder the routing process.

There are two types of Black hole Attack:

A. Single Black hole Attack

In single black hole attack, a single attacker node is present in the network. This Attacker node claims that, it has the shortest route to the destination, or it is the destination itself. And after the packet is routed through this attacker node, it drops the packet, and the packet never reaches the destination. A single black hole attack can take place, very easily in the mobile ad hoc networks.

B. Co-Operative/Collaborative Black hole Attack

In a Cooperative black hole attack, there are two or more black hole nodes present in the network. The cooperative black hole attack, takes place in two stages. In the first stage, the first black hole nodes, fakes to the network, that it has the shortest path to the destination, or it is the destination itself. After the packets have been routed to the attacker node, it forwards these packets to the second black hole node. Now this second black hole node, actually drops the packets. Due to this, cooperative black hole attacks are difficult to detect.

VIII. METHODOLOGY

For the detection and prevention of black hole, 2 different algorithms are been used. For detection of malicious node, Timer based baited system is used. And for Prevention of malicious node, 1-way hash function is used.

A. Detection of Malicious Node

For the purpose of detection of malicious node, Timer based baited algorithm is implemented. The algorithm is implemented as follows.

1) Step 1: The source node requests a route to the destination, by broadcasting the RREQ packets. The Malicious node gives a fake reply to the source mentioning that, it has the shortest route to the destination, or it is the destination itself, by sending the RREP packets. At the same time, the intended destination node also receives the RREQ packets from the source node, and so it will start a timer of fixed duration (say 1 second).
2) Step 2: The source then starts sending the packets to the malicious node, and the malicious node then drops the packets. Due to this the intended destination node will not receive any of the packets, and the timer will continue ticking on.
3) Step 3:After the fixed time duration, the destination node's timer will time-out, as it did not receive any packets. So, it send a packet to the source, mentioning that, it has not received any packets from the source. This packet will reach the source node, via another route in the network. This will alert the source node, that the packets sent by it, are been dropped.
4) Step 4:The source node will consider that, the node to which it is sending the packets, is suspicious. So, the source node will blacklist the node, to which it was sending the packets. The source node will broadcast this information, that the suspicious node is blacklisted, so that all other nodes in the network will blacklist the node, hence resulting in removing the malicious node from the network.

B. Prevention of Malicious Node

For the purpose of prevention of malicious node, 1-way hash function, md5 is implemented. The algorithm is implemented as follows.

1) Step 1: Every node in the network possess a unique Id, by the means of the hashing function.
2) Step 2: The source node generates a key pair, which is used for the authentication of the nodes, through which the packets is been sent. This key pair is then verified with the nodes in the network.
3) Stet 3: If the authentication is found invalid, the node is then marked as malicious node, and it is then removed from the network

IX. RESULTS

The NS2 scenario consists of a total of 20 node (node 0 to node 19), of which there is 1 source node (node 2), 1 destination node (node 3), and 1 attacker node (node 14). The communication is intended to be set up, between the source node and the destination node. To measure the performance of the network, different parameters like: Product Delivery Ratio (PDR), End-to-end Delay, Throughput and Energy, are been observed. The sending of packets begin at 1 second, simulation time.

The data is collected, based on 5 scenarios:

i) Without Black Hole (WOBH).
ii) With Black Hole (WBH).
iii) Detected Black Hole (DBH).
iv) Prevented Black Hole (PBH).
v) Detected-Prevented Black Hole (DPBH).

The graphs of PDR, Delay, Throughput and Energy are as follows:

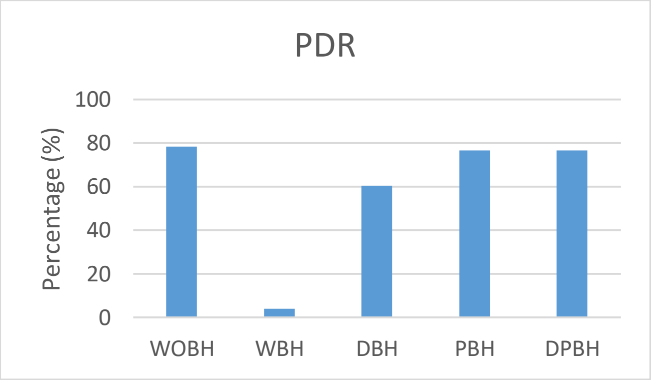

Fig. 1: PDR

PDR stands for packet delivery ratio .It is the ratio of number of packet delivered to the number of packets sent.As seen from the graph above the network without blackhole (WOBH) has the highest PDR of 78% while the network with Blackhole (WBH) has the least PDR of 4%. The network in which the Detection and Prevention methods are implemented (DBH, PBH, DPBH) has comparatively higher PDR than DBHwith 60%, 76% and 76% respectively. Higher PDR means, most of the sent packets are being delivered to the destination with minimum packet loss.

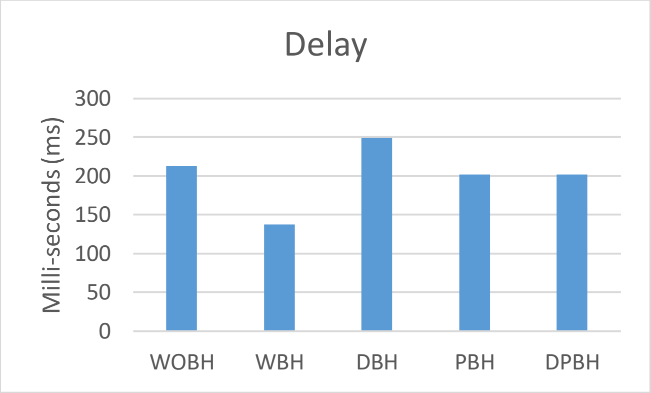

Fig. 2: Delay

Delay is the time taken by the packet to reach the destination from the source ,and is measured in Seconds.As seen from the graph above the network without blackhole (WOBH) has the the delay of 213ms, while the network with Blackhole (WBH) has the delay of 138ms. In WBH, the delay reduces significantly , as the packets are being dropped by the attacker node.

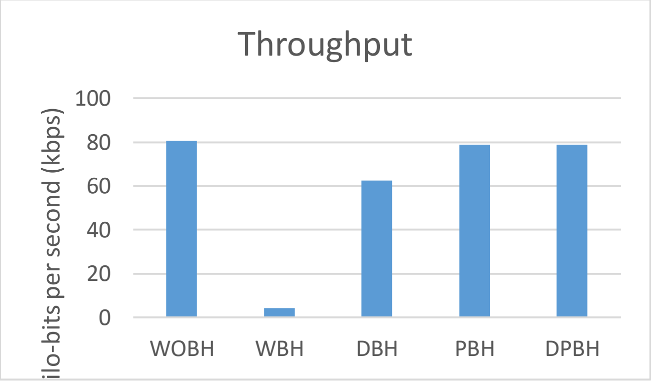

Fig. 3: Throughput

Throughput is the rate at which the packet are being sent through the network, from the source to the destination. As seen from the graph above the network without blackhole (WOBH) has the highest throughput of 80kbps, while the network with Blackhole (WBH) has the least throughput of 4kbps. In WBH, the throughput is the least , as the majority of the packets are being dropped by the attacker node, so very less packets actually reach the destination.

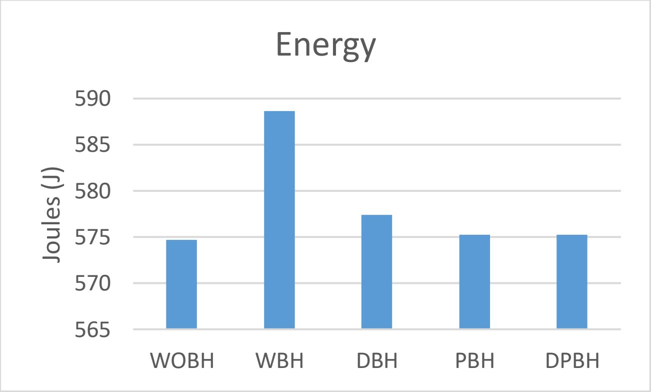

Fig. 4: Energy

Energy is the total enegy of the nodes in the network, packets has been transferred through the nodes.As seen from the graph above the network without blackhole (WOBH) has the least energy of 574J, while the network with Blackhole (WBH) has the highest energy of 588J. In WBH, the energy is high, because the energy of the node increases, whenever a packet is dropped by the attacker node.

X. CONCLUSION

MANET is vulnerable to various types of attack. Serious security problems in MANETs are - Black Hole attack. Black hole attack, is an attack where the malicious node sends fake RREP (route reply) to source node, claiming the false parameters and initiating the route discovery, and hence prevents the data traffic from the source node. Different existing techniques are used for detection of black hole attacks in MANETs is done. Each technique has their own merits and demerits. In the end, it is concluded that the effect of black hole attack is negative on the network, and the effect can be reduced by implementation of different prevention techniques. In future the algorithm can be made more effective, to reduce the effect of black hole attack in MANET.

REFERENCES

[1] Apurva Jain and AnshulShrotriya, “Prevention of Black Hole Attack on MANET Using Trust Based Algorithm”, International Journal of Scientific & Engineering Research, Volume 5, Issue 5, May-2014.

[2] Fan-Hsun Tseng, Hua-Pei Chiang and Han-Chieh Chao, “Black Hole along with Other Attacks in MANETs: A Survey”, J Inf Process Syst, Vol.14, No.1, pp.56~78, February 2018

[3] Nancy Mittal and Lal Chand, “Prevention and Detection Techniques under Black Hole Attack in MANETS: A Survey”, ISSN 0973-6972 Volume 10, Number 4 (2017), pp. 551-558.

[4] Monika Shivhare, Prof. Praveen Kumar Gautam, “A Literature Survey of Black hole Attack in MANET”, International Journal of Recent Trends in Engineering & Research (IJRTER) Volume 02, Issue 06; June - 2016 [ISSN: 2455-1457].

[5] Rashmi, AmeetaSeehra, “Detection and Prevention of Black-Hole Attack in MANETS”, International Journal of Computer Science Trends and Technology (IJCST) – Volume 2 Issue 4, Jul-Aug 2014.

[6] Veenita and Shamsher Singh Malik, “Detection and Prevention of Black Hole Attack in MANET”, International Journal of scientific research and management (IJSRM) ||Volume||4||Issue||09||Pages||4487-4493||2016||.

[7] NakkaNandini, Reena Aggarwal, “Prevention of black hole attack by different methods in MANET”, International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 4 Issue 2, February 2015.

[8] Aniruddha Bhattacharyya, Arnab Banerjee and Dipayan Bose, “Different types of attacks in Mobile ADHOC Network: Prevention and mitigation techniques”.

[9] Fan-Hsun Tseng, Li-Der Chou and Han-Chieh Chao, “A survey of black hole attacks in wireless mobile ad hoc networks”, Tseng et al. Human-centric Computing and Information Sciences 2011, 1:4.

[10] AdwanYasin and Mahmoud Abu Zant, “Detecting and Isolating Black-Hole Attacks in MANET Using Timer Based Baited Technique”, Wireless Communications and Mobile Computing Volume 2018, Article ID 9812135.

[11] Khushbu Patel, “SURVEY OF BLACKHOLE ATTACKS ON AODV PROTOCOL IN MANET”, International Journal For Technological Research In Engineering Volume 1, Issue 6, February-2014.

[12] Ahmed Ibrahim, Nagy E Zaki, “Solution to Black Hole Attack in Ad Hoc on Demand Distance Vector Routing Protocol”, Journal of Computer Sciences and Applications, 2015, Vol. 3, No. 4, 90-93.

[13] VipinKhandelwal and Dinesh Goya, “BlackHole Attack and Detection Method for AODV Routing Protocol in MANETs”, International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 2, Issue 4, April 2013.

[14] AmanSaurabh, RakeshYadav and Harjeet Kaur, “Identifying & Isolating Multiple Black Hole Attack on AODV protocol in MANET”, International Journal of Innovative Research in Science, Engineering and Technology Vol. 4, Issue 5, May 2015.

[15] NeelamJanak Kumar Patel and Dr. KhushbooTripathi, “Modified AODV Protocol for Detection and Prevention of Black hole Attack in Mobile Ad Hoc Network”, International Journal of Engineering Research in Computer Science and Engineering (IJERCSE) Vol 5, Issue 3, March 2018.