Technique to Detect and Isolate Multiple Black-Hole Attack by Phony Destination Request

Mr.R.A.Mukkawar[1], Prof. S.Y.Gawali[2]

[1]M.E Student, Computer Department, BNCOE, Pusad, INDIA
[2]Professor, Computer Department, BNCOE, Pusad, INDIA

Abstract - *MANET (Mobile Ad-hoc Network) is collection of wireless network establishing a network in which nodes communicate with each other by network systems such as the Internet. In such networks, nodes are able to move and synchronize with their neighbors. Due to mobility, connections in the network can change dynamically and nodes can be added and removed at any time. This work based mainly on the concept of MANET which is studied well and then the protocol regarding them is also studied. The AODV protocol will be used to find the shortest path in the network from source to destination. In our system while finding the shortest path, black hole attack is encountered and the aim of system is to remove this attack which resulting into the reduction of packet drop. For this one new technique is implemented in which the source will send the phony destination request i.e. fake destination node request in the network which is actually not present in network. And as per the working of black hole it will defiantly replay to that request by this way we will get the black hole. And if there is a presence of more than one fake node in the network so in that case obviously all these node will reply and this situation where more than one Black-Hole is working called as multiple black hole attack. Now the alarm message will be send into the network that is referring to those malicious nodes and now every genuine node is aware of these fake nodes and no single node will communicate with those nodes. So these will automatically goes out of network. Using this technique the throughput and pack loss is improved.*

***Key Words*: AODV Routing Protocol, Ad-hoc, Black hole, MANET, Worm hole.**

1. INTRODUCTION

We are living in the information age. Information is an asset that has a value like any other assets. As the information is distributed, information needs to be secured from attacks and needs to be hidden from confidentiality, integrity and availability. Wireless Networking is a technology in which two or more computers communicate with each other using standard network protocols wirelessly [1]. It can be either infrastructure or infrastructure-less. In infrastructure based network, communication takes place only between the wireless nodes and the access points. In infrastructure-less network, there is no pre-existing infrastructure such as routers in wired networks or access points in wireless networks. Ad-hoc network is an infrastructure-less network and thus decentralized type of wireless network. In ad-hoc network, every node participates in routing by forwarding data to all the nodes in the network and then determining dynamically, on the basis of network connectivity, the nodes which forward data [3].

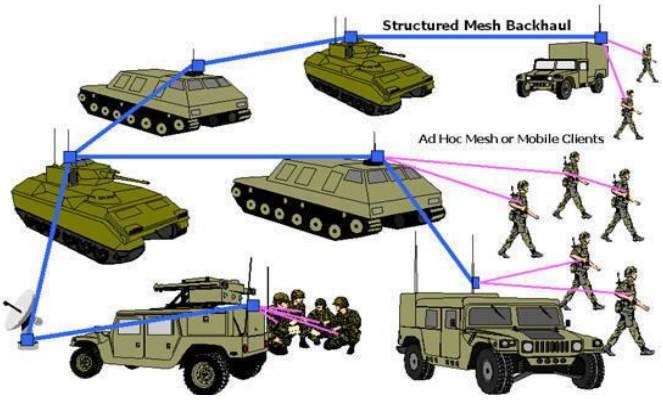

Fig-1: Example of mobile Ad-hoc network

MANET (Mobile Ad-hoc Network) is one of the types of Ad-hoc network. Every device in MANET is free to move by itself in all the directions. It can change its links to other devices frequently. The main challenge in building a MANET is making each mobile device capable to maintain the information which is necessary to route the traffic. A MANET is a collection of mobile nodes that can communicate with each other without the use of predefined infrastructure or centralized administration [2]. Since no fixed infrastructure or centralized administration is available, these networks are self-organized and end-to-end communication may require routing information via several intermediate nodes. Nodes can connect each other randomly and forming arbitrary topologies. Each node in MANET acts both as a host and as a router to forward messages for other nodes that are not within the same radio range. For deployment of MANETs several routing protocols have been proposed. The protocols differ in terms of routing methodologies and the information used to make routing decisions [6]. On the behalf of their different working methodologies, these routing protocols are divided into three different categories as Reactive Protocols, Proactive Protocols and Hybrid Protocols shown in fig 2.

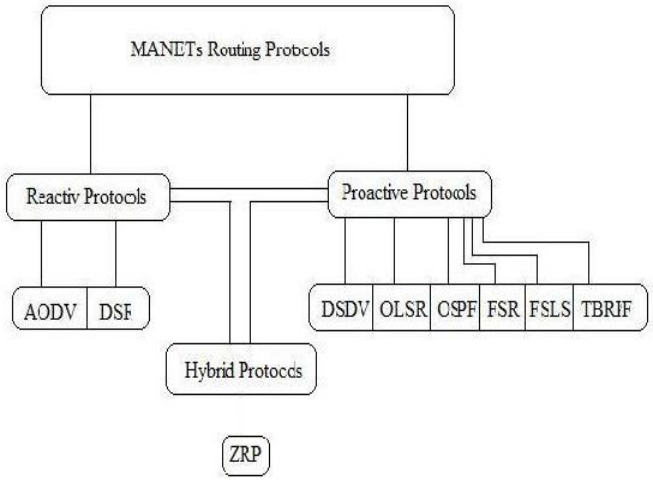

Fig-2: Categories of MANETs Routing Protocols

Proactive protocols, such as Optimized Link State Routing (OLSR) attempt to monitor the topology of the network in order to have route information between any source and destination available at all time. Proactive Routing Protocols are also called table driven routing protocols as all the routing information is usually kept in tables. Reactive routing protocols such as Ad hoc On Demand Distance Vector (AODV) find the route only when there is data to be transmitted and as a result, generate low control traffic and routing overhead. Hybrid protocols such as Gathering-based routing protocol (GRP) could be derived from the two previous ones, containing the advantages of both the protocols, using some quality of one type and enhancing it with the participation of the other one [5].

MANET has number of quantitative and qualitative metrics that can be used to evaluate the performance of the routing mechanism in network. There are various parameters for the purpose of evaluating the performance of the routing mechanism, as given below:

Packet Delivery Ratio

It is the ratio of the data packets delivered to the destination to those generated by the CBR sources. Packet Delivery ratio specifies the loss rate, which limits the maximum throughput of the network.

End-to-End Delay

It is the average end-to-end delay of the data packet, which includes all possible delays caused by buffering during route discovery, queuing delay at the interface, retransmission delays, at the mac, propagation and the transfer times. It indicates how long a packet took for a packet to travel from the source to the application layer of the destination.

Control Overhead

The number of the control packets transfer for maintaining the route of the transmission is said to be control overhead.

Normalized Routing Overhead

The total number of the routing packets transmitted for each delivered data packet is known as normalized routing overhead. Each hop-wise transmission of these packets is counted as one transmission.

Throughput

It is total number packets successfully delivered to the individual destination over total time divided by total time.

Energy consumption

It is the respective energy consumption of the node at the particular time, or can be calculated as average energy consumption for the particular data transmission in routing [11].

There are different types of attacker present in MANETs, which tries to reduce the performance of network. Various attackers are classified in the figure 1.2.

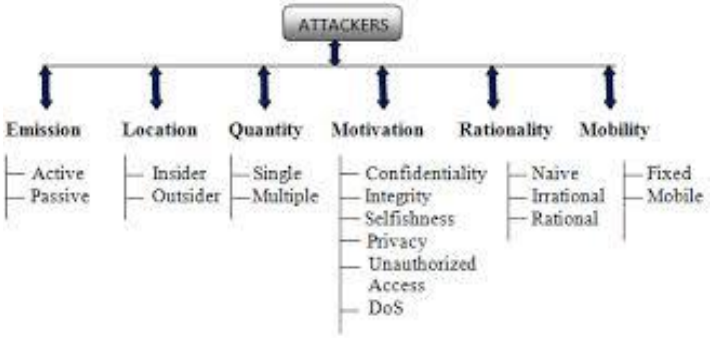

Fig-3: Classification of Attackers

Mobile Ad hoc networks are vulnerable to various attacks not only from outside but also from within the network itself. Ad hoc network are mainly subjected to two different levels of attacks. The first level of attack occurs on the basic mechanisms of the ad hoc network such as routing. Whereas the second level of attacks tries to damage the security mechanisms employed in the network.

The attacks in MANETs are divided into two major types. First is Internal Attacks this type of attacks are directly leads to the attacks on nodes presents in network and links interface between them. This type of attacks may broadcast wrong type of routing information to other nodes. Internal attacks are sometimes more difficult to handle as compare to external attacks, because internal attacks occurs due more trusted nodes. Traffic can be analyze between other nodes and may participate in the activities of other networks like black-Hole, selective packet drop attack etc.

Second type is External attacks these types of attacks try to cause congestion in the network, denial of services (DoS), and advertising wrong routing information. External attacks prevent the network from normal communication and producing additional overhead to the network. External attacks can classify into two categories: -

The characteristics of MANETs make them susceptible to many new attacks. These attacks can occur in different layers of the network protocol stack [9].

Table-1: Attacks on the Protocol Stack

Layer	Types of Attacks
Application	Malicious code, Data corruption, viruses and worms
Transport	Session hijacking attack, SYN Flooding attack
Network	Black-Hole, wormhole, Sinkhole, Link spoofing, Rushing Attack, Replay attacks, Link Withholding, Resource Consumption Attack, Sybil attack
Data Link	Selfish misbehaviour, malicious behaviour, traffic analysis
Physical	Eavesdropping, jamming, active interference

2. BLACK-HOLE ATTACK

In a Black-Hole attack, malicious node waits for neighboring nodes to send RREQ messages. When the malicious node receives an RREQ message, without checking its routing table, immediately sends a false RREP message giving a route to destination over itself, assigning a high sequence number to settle in the routing table of the victim node, before other nodes send a true one. Therefore requesting nodes assume that route discovery process is completed and ignore other RREP messages and begin to send packets over malicious node. Malicious node attacks all RREQ messages this way and takes over all routes. Therefore all packets are sent to a point when they are not forwarding anywhere. This is called a Black-Hole. If malicious node masquerades false RREP message as if it comes from another victim node instead of itself, all messages will be forwarded to the victim node. By doing this, victim node will have to process all incoming messages and is subjected to a sleep deprivation attack [10].

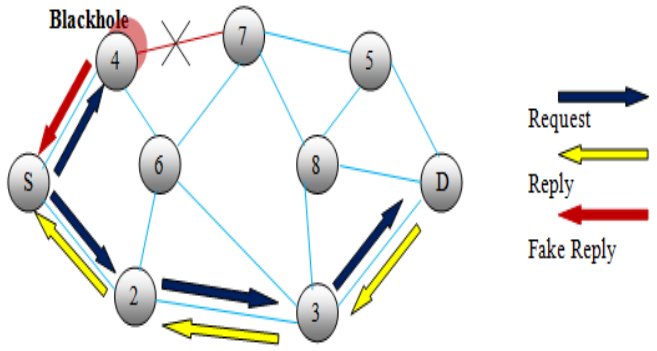

Fig-4: Black-Hole Attack

In above figure 4, malicious node "4" advertises itself in such a way that it has a shortest route to the destination. When source node "S" wants to send data to destination node "D", it initiates the route discovery process. The malicious node "4" when receives the route request, it immediately sends response to source. If reply from node "4" reaches first to the source than the source node "S" ignores all other reply messages and begin to send packet via route node "2". Now this node is Black-Hole Node that will be absorbing whole packet send by node "S". As a result, all data packets are consumed or lost at malicious node ultimately resulting into increase in throughput.

If there is one node is doing this then that will be the single type and if multiple nodes are doing this then that will be the multiple Black-Hole attack. As this kind of attack is difficult to find the most important type is this one [8].

Black hole Attacks are classified into two categories out of which first one is single Black Hole Attack. In Single Black Hole Attack only one node acts as malicious node within a zone. It is also known as Black Hole Attack with single malicious node. Another is Collaborative Black Hole Attack in Collaborative Black Hole Attack multiple nodes in a group act as malicious node. It is also known as Black Hole Attack with multiple malicious nodes.

3. PROPOSED WORK

Propose work is actually divided into two parts first is Black-Hole Detection and second is Black-Hole Avoidance. Following is the actual work flow of the system.

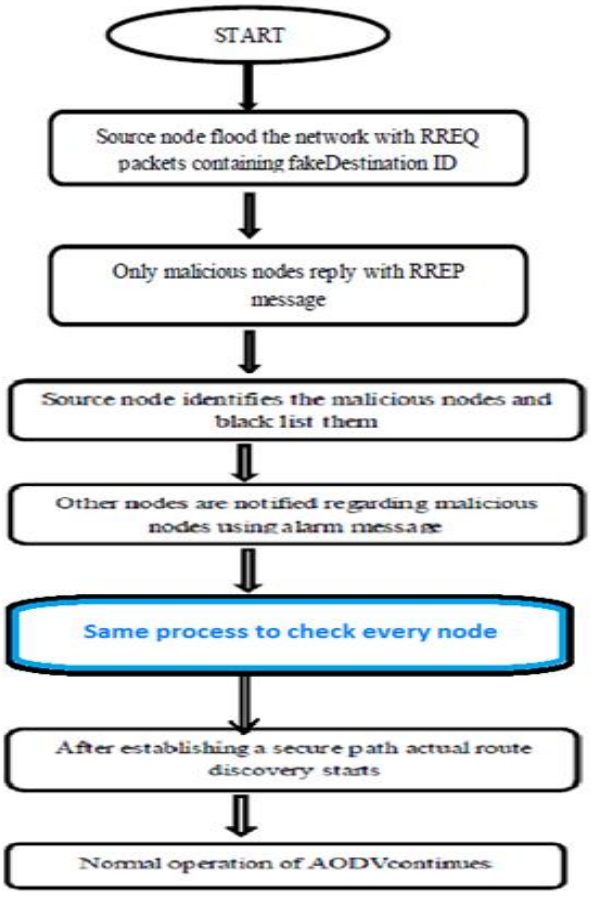

Fig-5: Flowchart of Proposed System

3.1. Black-Hole Detection

As per work flow to isolate Black-Hole attack from the network a new method is introduces in which source node floods the route request packets(RREQ) in the network with fake destination ID. As the malicious node does not know about any destination, it reverts back with route reply packet (RREP) and all legitimate (genuine) nodes will not revert back. The source node maintain table in which the information about the malicious nodes are stored. In this way the identification the malicious node is been done. This is the first phase where Black-hole is detected.

3.2 Black-Hole Avoidance

Now here the source node has identified the malicious node and the same process will continue until all malicious nodes will get identified. So now to isolate them from the network, source node will floods the network with ALARM message and the table which contain the information of malicious nodes. After receiving the ALARM message the intermediate nodes stop the communication with these malicious nodes. Now the source node again floods the network with RREQ message having genuine destination ID and select a reliable path to the destination. In this way the Black-Hole attack is avoided [11].

4. SIMULATION AND RESULT

We use NS-2 to form the simulation environment. The AODV protocol is used to detect black hole. The operating system used here is Fedora. The parameters that are considered to show the simulation are given below.

Simulation Parameters:
The following table describes the values of various parameters taken for performing the simulation.

Table-2: Result

Sr. No	Parameter	Value
1	Simulation Time	50s
2	Terra in Area	800 * 800
3	Application Traffic	CBR(Constant Bit Ratio)
4	Routing Protocol	AODV
5	Number of Nodes	15
6	Number of Source	1

SIMULATION PARAMETERS
Number of nodes: This parameter in the above table is used to represent number of nodes that are used for conducting the simulation.

Traffic type: Network traffic can be of two types viz. Variable Bit Rate (VBR) and Constant Bit Rate (CBR). The CBR traffic can suffer a maximum delay of T.
Simulation time: Simulation time is the duration of time for which the simulation is carried out.

Quantitative Metrics:
There are a number of quantitative metrics that can be used for evaluating the performance of a routing protocol for mobile wireless ad-hoc networks. The packet delivery ratio and throughput are most important for best-effort traffic. The packet delivery ratio is defined as the fraction of all the received data packets at the destinations over the number of data packets sent by the sources. This is a significant metric in networks. It is desired that the packet delivery ratio of the network should be high.
Packet Delivery Ratio = Total Data packets received/ Total Data packets sent.

C. Simulation Graphs:
In order to verify and evaluate the proposed protocol in a variety of scenarios, network simulations are inevitable. Here the implementation of the protocol is integrated with the ns-2 network simulator. The following figure shows the generated graphs for Throughput and Packet loss. In figure X-axis show time and y axis shows no. of packets. It is concluded that new technique has less packet loss as compare to previous one. It shows that after establishment of a secure route packet loss reduced by a large amount.

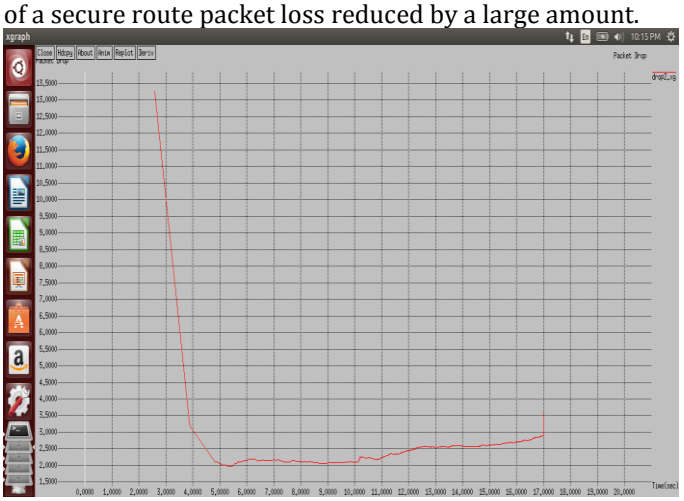

Fig-6: Graph of obtained Packet Drop

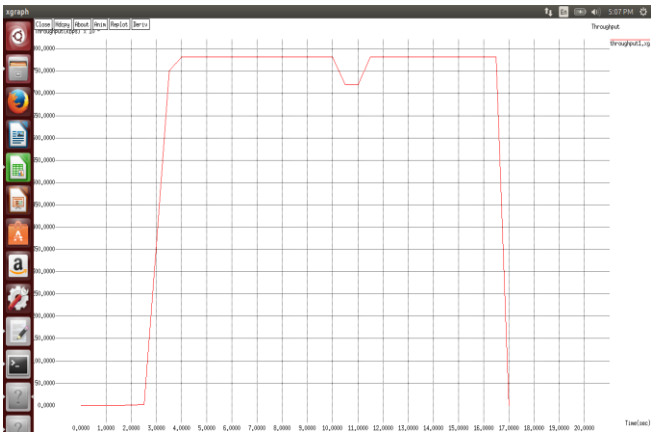

Fig-7: Graph of obtained Throughput

Table 2: Comparison Table

Parameter	Previous Scheme	Proposed Scheme
Throughput	60%	62.65%
Packet Loss	10%	3.8%

Table 2 presents the comparison between the previously described scheme and the proposed scheme. It is seen that the throughput of previous scheme is 60%, which is increased to 63% in the new technique proposed here. The packet loss is reduced to 4%, which was around 10% in old scheme.

7. CONCLUSION

Black hole attack is one of the most impotent security problems in MANET. It is an attack in which a node makes a prediction as genuine node and sends RREP to the node that initiated route discovery process, saying that it has the shortest and best route to the destination. In this way it consecutively deprives data packets from source node and drop them, which may result in dramatic degradation in the performance of an ad hoc network. In this paper, security issues in MANETs are discussed in general, and in particular multiple black hole attack has been described in detail. A security technique has been proposed, that can be used to identify the black hole nodes and isolate them from the network. The proposed scheme has been evaluated by implementing it in the network simulator ns-2.By using this proposed technique the packet loss is been reduced to less than 50% and throughput is also increased than previous technique. However, there is still much progress to be done to get higher throughput.

REFERENCES

[1]HimaniYadav, Rakesh Kumar, "A Review on Black Hole Attack in MANETs", International Journal of Engineering Research and Applications (IJERA), ISSN: 2248-9622, www.ijera.com, Vol. 2, Issue 3, May-Jun 2012, pp.1126-1131.

[2]Dr.Hariganesh P,JemimmaIlakiaNancy.C, "A Survey:Performance Analysis of Black Hole Attack In MANET", International Journal of Advancements in Research & Technology, Volume 3, Issue 6, June-2014 72 ISSN 2278-7763,pp 72-75.

[3] Anjaly Joy, SijoCherian, "Black Hole Attack and Itsmitigation Techniques in AODVand OLSR", International Journal of Computer Science & Engineering Technology (IJCSET), ISSN: 2229-3345, Vol. 4, No. 06, Jun 2013, pp. 740-745.

[4]Mehdi Medadian, Ahmad Mebadi, ElhamShahri, "Combat with Black Hole Attack in AODV Routing Protocol", Proceedings of the 2009 IEEE 9th Malaysia International Conference on Communications, 15 -17 December 2009, Kuala Lumpur Malaysia, pp. 530-535.

[5] MangeshGhonge, Prof.S.U.Nimbhorkar, "Simulation of AODV under Blackhole Attack in MANET", International Journal of Advanced Research inComputer Science and Software Engineering, Volume 2, Issue 2, February 2012, ISSN: 2277 128X, pp.657-661.

[6] Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, and Yoshiaki Nemoto, "Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method", International Journal of Network Security, Vol.5, No.3, pp.338–346, Nov. 2007.

[7]MamtaSengar, PawanPrakash Singh, SavitaShiwani, "Detection of Black Hole Attack In MANET Using FBC Technique", International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), Volume 2, Issue 2, March - April 2013, pp. 269-272.

[8] ShekharTandan and PraneetSaurabh, "A PDRR based detection technique for blackhole attack in MANET",International Journal of Computer Science and Information Technologies (IJCSIT), Vol. 2 (4), 2011, pp. 1513-1516.

[9] Gagandeep, Aashima, Pawan Kumar, "Analysis of Different Security Attacks in MANETs on Protocol Stack A-Review", International Journal of Engineering and Advanced Technology (IJEAT), ISSN: 2249 – 8958, Volume-1, Issue-5, June 2012, pp. 269-275.

[10] ChanderDiwaker, ChanchalAghi, Kulvinder Singh, "Detection and Prevention of Black hole Attack in MANET: A Review", International Journal of Emerging Technologies in Computational and Applied Sciences (IJETCAS), ISSN (Print): 2279-0047, 2013, pp. 294-297.

[11] Manisha Raj, Prof. Vishal Shrivastava, "A NewMethod to Identify and Isolate Multiple Black Hole Attack using Fake Route Request", International Journal of Advance Engineering and Research Development ISSN: 2348 – 6406,Volume 2, Issue 3, March -2015.