Scientific Journal of Impact Factor(SJIF): 3.134

e-ISSN(O): 2348-4470
p-ISSN(P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 2,Issue 3, March -2015

A NewMethod to Identify and Isolate Multiple Black Hole Attack using Fake Route Request

Manisha Raj[1], Prof. Vishal Shrivastava[2]

[1]M.Tech. Scholar, Comp. Sc. &Engg.,Arya College of Engg.& IT,Jaipur, India
[2]Professor, Comp. Sc. &Engg.Dept.,Arya College of Engg.& IT,Jaipur, India

Abstract—*In today's era, wireless communication is gaining popularity.With the features viz. dynamic topology, infrastructure-less and distributed management, MANET has engrossed many researchers to work on it. Nodes in the MANET can join or leave the network any time. Due to these characteristics, MANET is susceptible to many attacks. Thus its security is still the main issue of concern. One of the major attacks on MANET is called black hole attack, in which one or more malicious node forge the source by sending false reply message and attract the traffic towards themselves. In this paper, AODV routing protocol is considered to be attacked by black hole nodes. A novel technique is proposed here to detect and isolate black hole nodes in the network. For a secure path establishment between sender and receiver, Deffie-Hellman key exchange algorithm is used. The scheme is better in terms of packet loss and throughput. The simulation is done on ns-2.*

Keywords:*black-hole, throughput, routing algorithm, ad-hoc, malicious node, AODV.*

I. INTRODUCTION

The ad hoc network is a decentralized type of wireless network in which there is no central controller or access point. There is no pre-existing infrastructure such as routers in wired networks or access points in wireless networks on which it depends. The network is called ad-hoc as it is infrastructure-less. The ad-hoc networks are a new standard of wireless communication for moveable hosts. Basically it's a network which is used in critical situation/causes [1].

A mobile ad hoc network incorporate mobile devices such as cell phones, PDA's, laptops etc., that communicate with each other via intermediate nodes. MANET sets up a network whenever a transfer has to take place. There is no central control present to manage the communication and data transfer between mobile nodes. The transmission range of the nodes is limited so it uses multi hops to transfer data packets between the nodes which are out of range. MANETs are having the freedom to govern itself and act independently. The nodes in manet operates as host, when it wants to transit or receive data or router, when it is used just to forward packets to other nodes. There is no centralized system or node to manage the network scenario.[2]Manet does not pursue a fixed infrastructure as the nodes can anytime join or leave the network. They do not have to ask any node in the network to do this. The network manages the transfer of data in a cooperative way i.e. the intermediate nodes work in cooperative manner to forward the data packet to the destination. It is a self-configurable network i.e. nodes can work as host as well as router according to the circumstances. Due to the dynamic nature of MANET, routing of the data packets is more complex task. It has a constrained capability and less hardware resources.

Routing protocols are used to set up an optimal & effective route between participating entities. There are several routing protocols available for MANET which is classified into three categories namely proactive, reactive and hybrid. Hybrid is the combination of proactive and reactive protocol. Manet is useful where all the networks are out of reach like battlefields, disaster management, rescue missions & military applications. Security is still the complex issue in MANETs as it is infrastructure less, involves mobile nodes and deploys dynamic topology. Each routing protocol has security issues for which so many solutions are available but still there are some problems which are unable to prevent completely.[3,4]

One of the major attacks is black hole attack which is the well-known security threat in wireless ad-hoc networks.[3] This paper focuses on various types of black hole attack, their detection and solutions. Black hole attack can be broadly classified into ordinary and cooperative black hole attack.If more than one node is involved in attack, than it is known as cooperative black hole attack. Black hole is an active attack which is considered to be severe, thus many researchers have worked on it. These attacks are mainly evaluated on the basis of performance matrices including Packet Delivery Ratio (PDR), Packet Loss, Routing Overhead and Average delay.[2,10] In this paper we first discuss different types of attacks and we a new method is described to detect and isolate multiple black hole attack.

II. SECURITY GOALS

A. Availability

It is the ability of network to provide its services when required. The nodes should be available to provide their services irrespective of the security state of it. Denial of service attack is related to the availability of a node.[4, 9] Attacker can flood the network with large number of packets to degrade its performance and to make the services unavailable.

B. Confidentiality

Ensures certain information is never disclosed to unauthorized entities i.e. only the authorized people or node can access the information flowing in the network.

C. Integrity

It is related to the identity of the message. It ensures that the message received is not modified or corrupted by unauthorized nodes.

D. Authentication

It is a kind of verification that ensures the identity of the source of information. It assures that the participant nodes in the communication are genuine and not impersonators. Without authentication intruders can impersonate themselves as a genuine participant and thus access the data and information flowing in the network.

E. Non-repudiation

Ensures that the sending entity cannot deny having sent the message.

III. SECURITY ISSUES OF MOBILE AD-HOC NETWORKS

Because of some features of MANET like dynamic topology, Lack of central monitoring, limited bandwidth etc., it suffers from various security attacks like worm hole attack, black holeattack , replay attack, jamming attack etc.[1] Some of the security issues are discussed here:

A. Dynamic Topology

As the nodes are free to join or leave the network at any time, so there are more chances of change in routes, partitioning of network and packet loss.

B. Lack of centralized management

MANET is an infrastructure less network which does not have any centralized management system which makes it more vulnerable to attacks.[1] Thus detecting and monitoring attacks is very difficult.

C. Limited bandwidth

Wireless network has lower bandwidth capacity then wired networks.

D. Limited Battery Power

In MANET, the only available energy source is battery power which is limited in mobile devices.

E Limited physical security

Because of the mobility of nodes MANET suffers from big security risks like eavesdropping, spoofing etc.

IV. BLACK HOLE ATTACK

Inthefigure 1,consideramaliciousnode M.When node1broadcasts aRREQpacket;nodes2,4and Mreceive it. Node M,beingamaliciousnode, doesnotcheckitsroutingtableforthe requestedroute tonode5.Hence, itimmediately sends backafalseRREPpacket, claiminga shortestroute tothedestination. Node 1 Receives the RREPfrom Maheadofthe RREPfrom 2and 4.Node 1 assumesthat the route throughM is the shortestroute and sends data packets to the destinationthrough it. When thenode1sends datatoM,itabsorbsallthe data anddropsthis data. As thisdata cannot reachtothe destinationitiscalledasaBlackholeattack.

Therefore, source and destinationnodes areunableto communicatewitheachother.The malicious node always sends RREP as soon as it receives RREQ withoutperforming standardAODVoperations,while keeping the Destination Sequencenumberveryhigh.[7]SinceAODVconsiders RREPhavinghighervalue of destinationsequencenumbertobefresh, theRREPsent by the maliciousnode istreatedfresh.[3]Thus, malicious nodes succeedininjecting BlackHoleattack. In this way the source node forged by the malicious node. The black hole is called an active type of attack, as it attracts the data packet towards itself and prevents the information reaching to the intended destination.

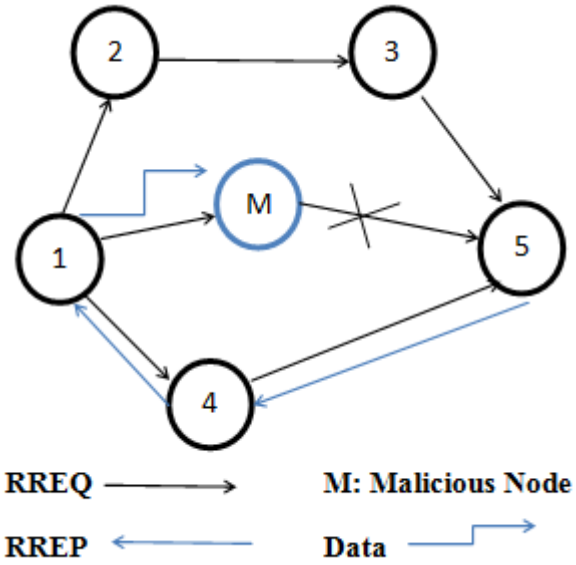
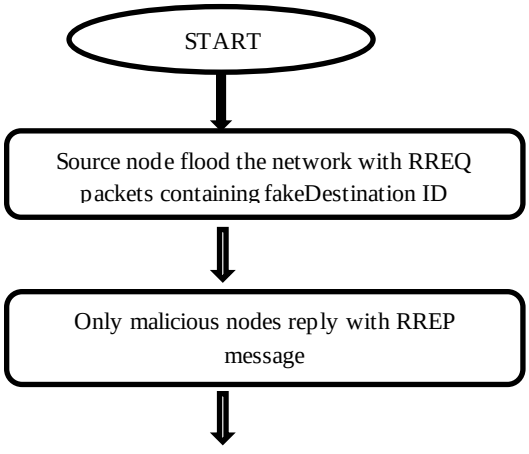


Fig.1Black HoleAttack

V. PROPOSEDWORK

The mobile ad-hoc network is the self-configuring type of networks in which the mobile nodes can join or leave the network when they want. It is a decentralized network in which source node can communicate to the destination node. The path between source and destination is required to be the shortest and reliable. AODV routing protocol is required to select the shortest and reliable path. To start the communication the source node floods the network with route request packets (RREQ).[3] The nodes which have direct path to the destination, reply to the source by using route reply packets (RREP). After receiving RREP message the source node select best path on the basis of hop count and sequence number. Some malicious nodes exist in the network which do not have path to destination but revert back with route reply packets. The source node may select the best path through that malicious nodes and that node may drop all the packets, which reduce the network throughput. These malicious nodes are known as black hole and this type of attack is called black hole attack.

To isolate black hole attack from the network a new method is introduces in which source node floods the route request packets in the network with fake destination ID. As the malicious node does not know about any destination, it reverts back with route reply packet and all legitimate (genuine) nodes will not revert back. The source node maintain table in which the information about the malicious nodes are stored. The source node identifies the malicious nodes and to isolate them from the network, it 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. To verify the reliability of selected path Diffie-Hellman key establishment algorithm is used. In the Diffie-Hellman algorithm if two parties, say, Master and Slave desires to interchange data, both agree on a symmetric key. A symmetric key is used to encrypt and decrypt the messages. Both the parties choose their own random number. On the basis of the selected random numbers, a secure channel is established.



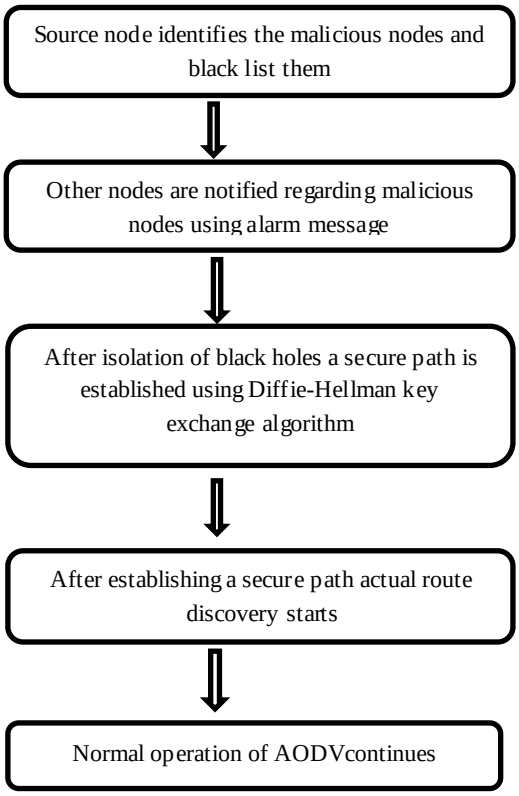


Fig. 2. Procedure for Detecting and Isolating Black Hole Nodes

V. SIMULATION

We use NS-2 to form the simulation environment. The AODV protocol is used to detect black hole. The operating system used here is Ubantu.[5] The parameters that are considered to show the simulation are given in Table 1.

A. Simulation Parameters

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

S. No.	Parameter	Value
1.	Simulation Time	50 s
2.	Terrain Area	800m X 800m
3.	MAC Type	802.11
4.	Application Traffic	CBR(constant bit Rate)
5.	Routing Protocol	AODV
6.	Data Payload	512 Bytes/Packet
7.	Pause Time	2s
8.	Number of Mobile Nodes	15
	Number of Sources	1
9.	No. of Adversaries	1 to 3

TABLE 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.

Pause time: this parameter represents the time interval for which the nodes can be paused in the network during 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.

B. 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. Here, we follow the general ideas described in RFC 2501, and we use four quantitative metrics. The packet delivery ratio and average end-to-end delay and throughput are most important for best-effort traffic.

- *Packet Delivery Ratio*

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

- *Average End-to-End Delay*

End-to-end delay includes all possible delays in the network caused by route discovery latency, retransmission by the intermediary nodes, processing delay, propagation delayand queuing delay. To average the end-to-end delay we add every delay for each successful data packet delivery and divide that sum by the number of successfully received data packets. This metric is important in applications in which delay cannot be considered such as video and voice transmission. The end-to-end delay is desired to be low.
Average End to End Delay = $\sum$ (Time received - Time sent)/ Total Data packets received

- *Overhead*

Ad hoc networks are designed to be scalable i.e. network size (no. of nodes) should not be predefined. As the network grows, various routing protocols perform differently.[4] The amount of routing traffic increases as the network grows. A significant measure of the scalability of the protocol, and thus the network, is its routing overhead. It is stated as the total number of routing packets transmitted over the network, expressed in bps (bits per second) or packets per second.[6] The desired overhead of a network should be low.

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.
First, packet loss is evaluated. In figure 3 red line shows packet loss in previous technique without security and green line shows packet loss in proposed technique.[8] 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.

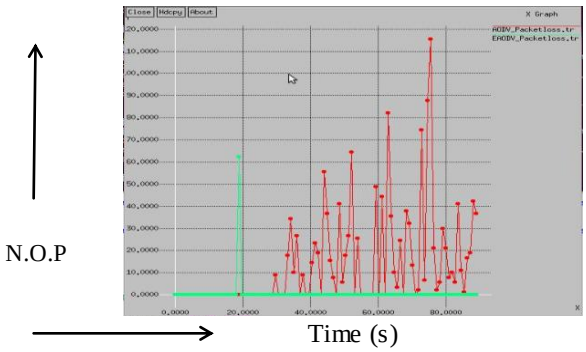


Fig. 3. Packet loss comparison

Next, we examine the throughput of the network and observed that the throughput of the proposed technique is better than the previous scheme. It is seen by the graph that the throughput of previous scheme was very high initially, but after a specific point it is reduced to zero because of the presence of black hole nodes in the network. But in our scheme the throughput of the network is better than the previous scheme.

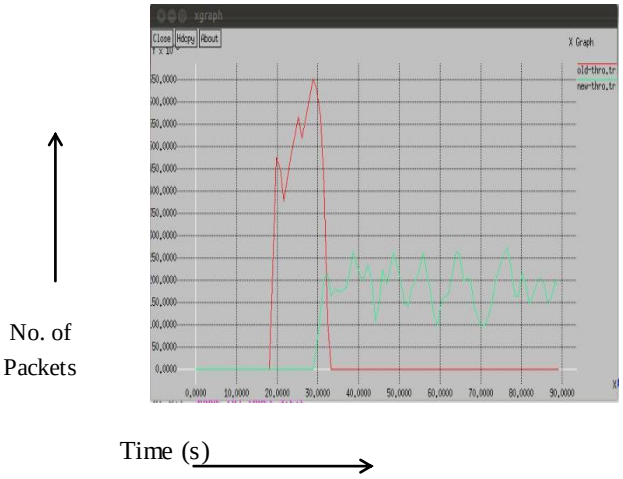


Fig. 4. Throughput comparison

Parameters	Previous Scheme	Proposed Scheme
Packet Loss	50%	10%
Throughput	18%	60%

TABLE2
COMPARISON TABLE

Table 2 presents the comparison between the previously described scheme and the proposed scheme. It is seen that the throughput of previous scheme is 18%, which is increased to 60% in the new technique proposed here. The packet loss is reduced to 10%, which was around 50% in old scheme.

VI. CONCLUSION

Black hole attack is one of the most essential security problems in MANET. It is an attack in which a node impersonates as genuine node and sends forged 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, and the results reveal the effectiveness of the mechanism.

REFERENCES

[1] Himani Yadav, 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, Sijo Cherian, "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 RoutingProtocol". 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-basedMobile Ad Hoc Networks by Dynamic LearningMethod", International Journal of Network Security, Vol.5, No.3, PP.338–346, Nov. 2007

[7] MamtaSengar, Pawan Prakash Singh, Savita Shiwani, "Detection of Black Hole Attack In MANETUsing 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 blackholeattack in MANET", (IJCSIT) International Journal of Computer Science and Information Technologies, 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

