IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 18, Issue 3, Ver. III (May-Jun. 2016), PP 68-72
www.iosrjournals.org

Prevent and Isolate Black Hole Attack in Manet Using Alarm Packets

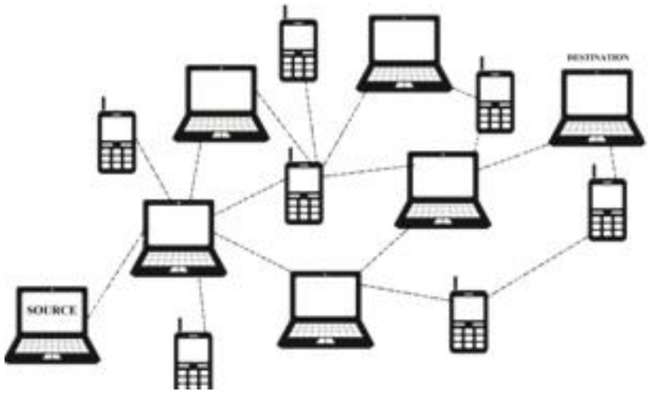
Sushmita Mahajan[1], Sanjeev Dhiman[2],
Student[1], Assistant Professor[2], Department of CSE,DAV University, Jalandhar

Abstract: *A mobile ad hoc network can be described as a wireless network which is a collection of heterogeneous mobile devices and is self-organizing, self-configuring. The security in MANET is a highly preferred research area these days because it is susceptible to various attacks like black hole attack which we are discussing in this paper. Due to black hole attack network performance degraded. In this paper we will propose new technique based upon alarm message to isolate and prevention of black hole attack.*

Keywords: *MANET, Black hole attack, alarm nodes, fake packets*

I. Introduction

A MANET (mobile ad hoc network) can be described as a wireless network which is a collection of heterogeneous mobile devices and is self-organizing, self-configuring. In this type of network the devices communicate through a wireless medium with each other [2]. The devices in the network should cooperate with each other so the packets can be transmitted via intermediate devices when there is no direct path from source to destination [3]. There is no concept of central controlling authority & a permanent network infrastructure in a mobile ad-hoc network. Transfer of packets is done with the help of routing protocols, which help in determining the suitable route from source to destination for initiating as well as maintaining a connection between the two. Network topologies are dynamic in nature, due to which there are link breakage and disruption in peer to peer connection



.

Fig.1 Mobile Adhoc Network

An ad hoc network is a wireless network describe by the nonexistence of a centralized and fixed infrastructure as displayed in Figure1. In the absence of an infrastructure in ad hoc networks poses great challenges in the functionality of these networks [4]. Therefore, we refer to a wireless ad hoc network with mobile nodes as a Mobile Ad Hoc Network. In a MANET, mobile nodes have the capability to accept and route traffic from their intermediate nodes towards the destination [5]. Therefore they can act as both routers and hosts. More frequent connection fading and re-associations place an energy constraint on the mobile nodes. The security and reliability are the other major challenges of MANET. In this, certain types of internal and external attacks are possible. The attacker node can join the network at any time and trigger the attack. It has been a tedious task to design the key management and self authentication mechanism for MANET.

II. Security Attacks in MANET:

There are many attacks in MANET. These are discussed as follow:

Wormhole attack:

Wormhole attack is performed by the malicious node which is inside or outside the network. Malicious node receives the data packets from one side of the network and redirects the whole network traffic to the other side. This attack leads to the exaggeration of delay in the network. Jamming Attack: The jamming attack is the active type of attack. Malicious nodes can send unlimited number of packets
to the selective node. The node will be unable to handle such large number of packets. In lieu of this, network blockage kind of situation has been cropped up.

Man-in-the-Middle Attack:

In MITM attack, attacker sits between the two communicating parties. The attacker can sniff any information of sender and receiver. Thus getting hold over the information being transmitted by the sender to the receiver. The attacker may launch a queue of other attacks viz interception, masquerading fabrication, once getting the information available at his dispense [7].

Denial-of-Service Attack:

When the Denial-of-service attack is successfully triggered by the attacker. The legitimate nodes are unable to access the required service. This is in lieu of the context that the legal sources have been over whelmed by the illegal users via the sending of large burst of packets on the behalf of legitimate users [8]. Thus overcrowding the resources, which in turn leads to disruption of services and hence drop down of network performance measurement parameters viz throughput and bandwidth to null value.
In this paper, we will discuss about black hole attack and its prevention measures.

III. Literature Survey

Sanjay Ramaswamy, et al proposed the solution for identifying multiple black hole nodes [6]. The solution is based on the modified AODV protocol by presenting the cross checking and data routing information table (DRI). In which the table is maintained for every single entry of the node. For the transfer of the packets the authors relied on the trusted nodes. In this paper, a defense mechanism is presented against the collaborative black hole attacks, our research is the extension of the secure algorithm proposed by S.Sankara Narayanan et.al [13]. This method makes use of the MAC address of the destination to validate each node in its path thereby providing a direct negotiation for secure route. The proposed scheme simulation is carried out to present the strength of the mechanism in mitigation of black hole attack while maintaining a fair level of packet delivery ratio, throughput and end to end delay in the network. Some enhancement in the existing AODV protocol is introduced by Latha Tamilselvan et al [1] which are capable to refrain cooperative black holes. The multiple black holes are cooperating with each other in this attack. The safe route should be discovered by refraining from the attacks. An assumption was made by the researchers while giving the solution for the concerned issue is the nodes are pre-authenticated and it can take part in the communication passage. The protocol uses Fidelity table in which all the node that is participating in the communication has a loyalty level that is used for checking the trustworthiness of the node. In the fidelity table, if any node have 0 value then it is perceived as malicious node and it will be removed. An intrusion detection using anomaly detection (IDAD) is introduced by Yibeltal Fantahun Alem et al to prevent the single and multiple black hole attacks [7]. It works on the principle that the nodes doesn't believe on the other nodes to forbid intrusion. IDAD consists of audit data which is the pre-collected set of anomaly actions. If the action (activity) of a node is identical to the actions then the system forbids the particular node. On simulating the proposed system, it is observed that it maximizes the network performance by reducing the control packets generation. The highest level routing methods are discussed by Fan-Hsun et al. They classified the proposals into a black hole attack and collaborative black hole attack and analyzed the solutions for those attacks and also provided a similarities between them. They presented summary of the advantages and disadvantages of the routing protocols used in wireless MANET [9]. An algorithmic approach for improving the security of AODV protocol is introduced by Rajib Das et al with the ability to identify and remove the black hole nodes in MANET [5]. An extra (additional) route is proposed to the intermediate node and it can send RREP message to the source node for discovering the path to the destination node is present or not. The proposed approach cannot be used to identify a cooperative black hole attack consists of many malicious nodes. Along with the routing table there is a data routing information (DRI) table which can be used for recognizing multiple black hole nodes. On simulating the proposed algorithm, it is observed that there is reduction in network throughput and packet delivery ratio.

IV. Black Hole Attack In MANET

In black hole attack, the requests are listened by the attackers. When a route request message is received by the attacker to the destination node for a path establishment, it creates a reply with the smaller route and enters into the path to drop the packets received by the attacker node [6]. In MANET, broadcast requests for route discovery are listened by an attacker. When a route request message (RREQ) is received by the attacker node for a route to the destination node, it creates a (RREP) route reply message with the short route and enters. into the path to drop the packets received by the node. The source node presumes that the destination node is down the black hole node and dumps the other (RREP) messages coming from the other nodes in the network. Now, source node begins to send the packets to the black hole node confiding that these packets will reach the destination node. Hence the black hole node draws the packets from the source node and instead of transmitting those packets to the destination node it will discard those packets. Thus the packets drawn by the black hole node will not reach the destination node.

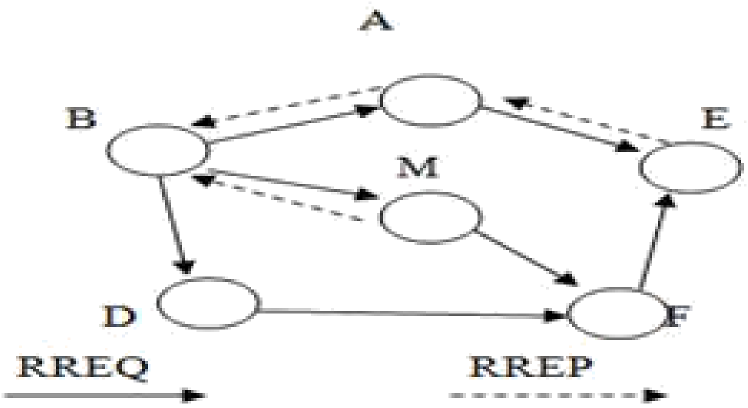


Fig.2 Routing Discovery Process in AODV

Black Hole problem can be explained as the process of exploiting a routing protocol by a malicious node by representing that it has the shortest path to the desired destination, instead of forwarding packets to its neighbors it drops the routing packets. From the figure2 let us assume that M is a malicious node. In the above figure node A is the source node & node E is the destination node, which A is trying to reach. So that it transmits the RREQ packet to all its neighbors “B” “D” and “M” respectively. As we know that M is a malicious node, it replies with a RREP packet as soon as it receives the RREQ packet, it declares that it has the shortest route to the destination without checking its routing table [10]. Therefore, the source node will receive the first RREP from M & after that from the other nodes in the network. On the basis of the RREP sequence received by A, it will believe that M has the shortest path to the desired destination E & it can transmit packets via M to reach the destination E. M being a malicious node will consume all the packets received by it which is required to be transfer to E [11]. Hence we can say that M is a Black Hole Node.

V. Proposed Technique

Among all the attacks discussed previous black hole attack is the most common active type of attacks. Black hole attack is the denial of service attacks which is triggered by the malicious nodes in the network. In the previous times, many techniques have been proposed to isolate black hole attacks from the network. When black hole attack is triggered in the network, throughput of the network reduced and delay increase as steady rate. The black hole attack is even worse if the multiple black hole nodes exist in the network. When multiple black hole nodes exist in the network, all the malicious nodes are responsible for triggering the black hole attack. This type of attack is called multiple black hole attack. In our work, we work on to detect and isolate multiple black hole attack in mobile Ad hoc network. First of all, we will deploy finite number of nodes in the network. After that path will established on the basis of AODV. Source will send fake route request packets to the network. The node which will be malicious send route reply packet to the network. In this way we will detect the entire malicious nodes which trigger black hole attack. After this for more security, we will again send alarm nodes from source. It will again isolate black hole attack after receiving alarm nodes. In third step will apply Diffie- Hellman algorithm to check the reliability of the selective path. In this way, we will isolate black hole attack. The whole scenario will be implementing on NS2 simulator.

VI. Experimental Results

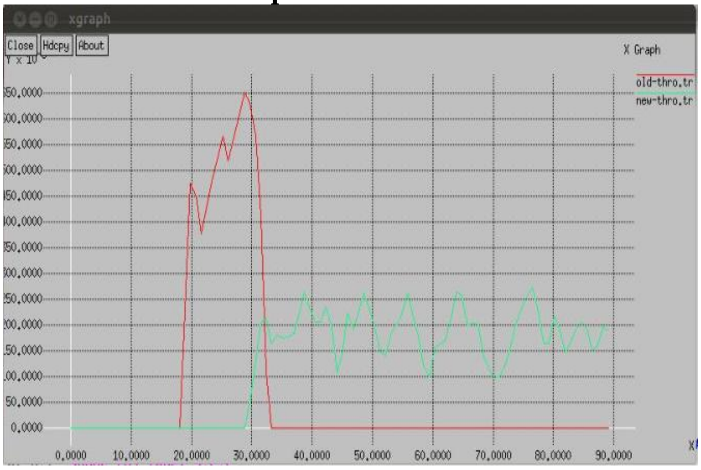


Fig.3 Throughput Graph

In above figure3 red line shows old throughput and green line show new throughput. X-axis shows time and y axis shows packets. It concluded that new technique has more throughput as compare to old technique.

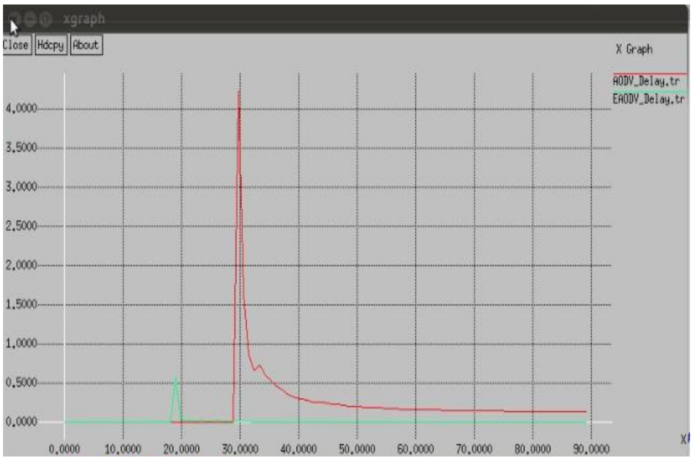


Fig.4 Delay Graph

In above figure 4 red line shows old delay and green line show new delay. X-axis show time and y axis shows packets. It concluded that new technique has less delay as compare to new technique. It proves that new technique is better than old technique.

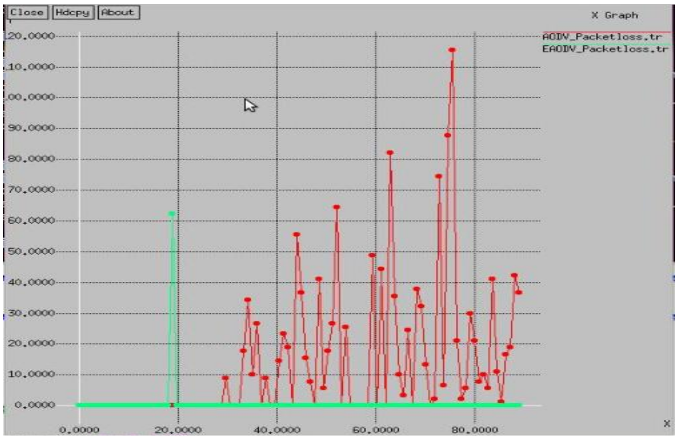


Fig.5 Packet Loss Graph

In above figure5 red line shows packet loss and green line show new packet loss. X-axis show time and y axis shows packets. It concluded that new technique has less packet loss as compare to new technique. It proves that new technique is better than old technique.

VII. Conclusion

As MANET being infrastructure less it can be deployed with fewer efforts as compared with the traditional network infrastructure environment. It has a lot of potential but still there are some issues to overcome. One of the popular research areas nowadays is security in MANET and in our thesis we are addressing security issues in one of the reactive routing protocol (AODV) in MANET. In this paper we will propose new technique to isolate and detect black hole attack to improve network performance.

References

[1]. Latha Tamilselvan and V Sankaranarayanan “Prevention of Co-operative Black Hole Attack in MANET”, JOURNAL OF NETWORKS, VOL. 3, NO. 5, MAY 2008.

[2]. Mohammad Al-Shurman and Seong-Moo Yoo “Black Hole Attack in Mobile Ad Hoc Networks”, ACMSE"04, April 2-3, 2004.

[3]. Priyanka Goyal, Vinti Parmar and Rahul Rishi “MANET: Vulnerabilities, Challenges, Attacks, Application”, IJCEM International Journal of Computational Engineering &Management, Vol. 11, January 2011.

[4]. Durgesh Wadbude and Vineet Richariya “An Efficient Secure AODV Routing Protocol in MANET”, International Journal of Engineering and Innovative Technology (IJEIT) Volume 1, Issue 4, April 2012

[5]. Rajib Das, Bipul Syam Purkayastha and Prodipto Das “Security Measures for Black Hole Attack in MANET: An Approach”.

[6]. Sanjay Ramaswamy, Huirong Fu, Manohar Sreekantaradhya, John Dixon and Kendall Nygard “Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks”.

[7]. Yibeltal Fantahun Alem and Zhao Cheng Xuan “Preventing Black Hole Attack in Mobile Ad-hoc Networks Using Anomaly Detection”, 2010 2nd International Conference on Future Computer and Communication.

[8]. Jaydip Sen, Sripad Koilakonda and Arijit Ukil “A Mechanism for Detection of Cooperative Black Hole Attack in Mobile Ad Hoc Networks”

[9]. Fan-Hsun Tseng1, Li-Der Chou1 and Han-Chieh Chao “A survey of black hole attacks in wireless mobile ad hoc networks”, Computing and Information Sciences 2011

[10]. Songbai Lu, Longxuan Li, Kwok-Yan Lam and Lingyan Jia “SAODV: A MANET Routing Protocol that can Withstand Black Hole Attack”, 2009 International Conference on Computational Intelligence and Security.

[11]. Sheenu Sharma, Roopam Gupta “SIMULATION STUDY OF BLACKHOLE ATTACK IN THE MOBILE AD HOC NETWORKS”, Journal of Engineering Science and Technology Vol. 4, No. 2 (2009) 243 – 250

[12]. S.Sankara Narayanan and S.Radhakrishnan , “Secure AODV to Combat Black Hole Attack in MANET” , 2013 International Conference on Recent Trends in Information Technology (ICRTIT)