Detect and Isolate Black hole attack in MANET using AODV Protocol

Jaspinder Kaur,Birinder Singh

***Abstract*-In AODV routing protocols many loop hole are there, these loop holes can gave arise to different type of active and passive attacks which are triggered by various inside and outside malicious nodes. Among all the type of attacks, black hole attack is the most common of attack which is possible in AODV protocol. Black hole attack is the denial of service attack. In this paper, we are proposing modifications in traditional AODV protocol to prevent black hole attack. The basic idea to detect and isolate malicious nodes is which the use of fake messages. The technique has been implemented in NS2 and a result of new technique has been compared with the existing techniques.**

***Index Terms* - Reactive, Proactive, Black hole, Denial of service, inside and outside**

I. INTRODUCTION

A wireless ad-hoc network consists of a collection of "peer" mobile nodes that are capable of communicating with each other without help from a fixed infrastructure or any centralized administration. There is no stationary infrastructure or base station for communication. Each node itself acts as a router for forwarding and receiving packets to/from other nodes. In ad hoc networks, the mobile nodes on the network dynamically establish the routing process by themselves. There is the possibility of more security threats in case of mobile and ad hoc networks (MANET) as compare to centralized wireless networks. A mobile ad-hoc network (MANET) is a self-configuring infrastructure less network of mobile devices connected by wireless. Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be a router. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic. Mobile Ad hoc Network (MANET) is a collection of independent mobile nodes that can communicate to each other via radio waves. The mobile nodes that are in radio range of each other can directly communicate, whereas others need the aid of intermediate nodes to route their packets. These networks are fully distributed, and can work at any place without the help of any infrastructure. This property makes these networks highly flexible and robust. There are a variety of attacks possible in MANET. The attacks can be classified as active or passive attacks, internal or external attacks, or different attacks classified on the basis of different protocols. A passive attack does not disrupt the normal operation of the network. The attacker only snoops the data exchanged in the network without altering it. It includes Eavesdropping, jamming and traffic analysis and monitoring. In case of active attacks, the attacker attempts to alter or destroy the data being exchanged in the network. This attack disrupts the normal functioning of the network. Active attacks can be internal or external. External attacks are carried out by nodes that do not belong to the network. Internal attacks are from compromised nodes that are part of the network. Since the attacker is already part of the network, internal attacks are more severe and hard to detect than external attacks .The ultimate goals of the security solutions for MANETs is to provide security services, such as authentication, confidentiality, integrity, authentication, non-repudiation, and availability to mobile users.

The literature Review is discussed in section 1. In section 2 various types of attacks in mobile ad hoc network is presented. AODV protocol and Black hole attack is written in section 3 .In section 4 new

proposed technique is illustrated . Results are shown in section 5. In last section 6 future work and conclusion is written

II. LITERATURE REVIEW

Hongmei Deng, Wei Li, and Dharma P.Agarwal [1] proposed the method for detecting the single black hole node. In this proposed method, each intermediate node send backs the next hop information when it sends back an RREP message. When the source node receives the reply message from intermediate node, it does not send the data packets quickly, but it extracts the next hop information and then sends the Further-Request to the next hop to verify that it has the route to the intermediate node. If the next hop has no route to the inquired intermediate node, but has a route to the destination node, we discard the reply packets from the inquired intermediate node, and use the new route through the next hop to the destination. At the same time, send out the alarm message to the whole network to isolate the malicious node. Satoshi Kurosawa et al [2] proposed the solution emphasis on the dynamically changing conditions of ad hoc networks. In AODV, the destination sequence is used to determine the freshness of the routing information contained in the message from originating node. The attacker must generate its RREP with the destination sequence number greater than the destination sequence number of the destination node. It is possible to for the attacker to find the destination sequence number from the RREQ packet. But if other nodes attempts to construct the route to the destination node other than the source node, then the destination node's sequence number will be significantly different from the current destination sequence number**.** Payal N. Raj et al [3] proposed DPRAODV (detection, prevention and reactive AODV) to prevent the black hole attack by informing the other nodes about the malicious node. As the value of RREP sequence number is found to be higher than the threshold value, the node is suspected to be malicious and it adds the node to the black list. As the node detected an anomaly, it sends a new control packet, ALARM to its neighbors. The ALARM packet has the black list node as a parameter so that, the neighboring nodes know that RREP packet from the node is to be discarded. Further, if any node receives the RREP packet, it looks over the list, if the reply is from the blacklisted node; no processing is done for the same. The threshold value is the average of the difference of destination sequence number in each time slot between the sequence number in the routing table and the RREP packet. Yiebeltal Fantahun Alem et al [5] proposed an Intrusion Detection using Anomaly Detection (IDAD) is a system for detecting computer intrusions and misuse by monitoring system activity and classifying it as either normal or anomalous. IDS can be classified as Network-based and Host-based. Network-based IDS can be installed on data concentration points of a network such as switches and routers. Where as Host-based IDS are installed on hosts so that they can supervise the activities of a host and users on the host.

III. BLACK HOLE ATTACK IN AODV

A black hole problem means that a malicious node utilizes the routing protocol to claim itself of being the shortest path to the destination node, but drops the routing packets but does not forward packets to its neighbors. Imagine a malicious node 'M'. When node 'A' broadcasts a RREQ packet, nodes 'B' 'D' and 'M' receive it. Node 'M', being a malicious node, does not check up with its routing table for the requested route to node 'E' [6]. Hence, it immediately sends back a RREP packet, claiming a route to the destination. Node 'A' receives the RREP from 'M' ahead of the RREP from 'B' and 'D'. Node 'A' assumes that the route through 'M' is the shortest route and sends any packet to the destination through it. When the node 'A' sends data to 'M', it absorbs all the data and thus behaves like a 'Black hole'.

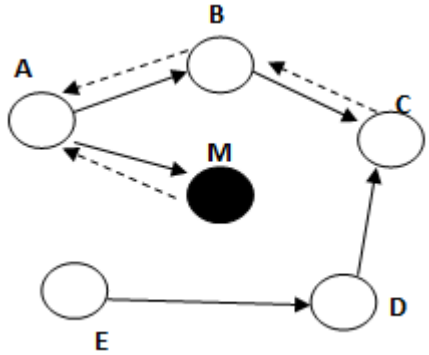

Fig1. Black Hole Attack in AODV protocol

IV. NEW PROPOSED TECHNIQUE

In MANET, nodes are self-configuring so it can move freely in any direction. There is no central controller in MANET. Security of the MANET is a big issue. Different types of attacks are possible in MANET. There can be some internal attack or external attacks. Internal attack affects the network internally. With the help of any malicious node it can be done. External attacks affect the network externally. The black hole attack is the most common type of attack which is triggered by malicious node which is present in the network. In this work, new technique has been proposed which detect the malicious node and isolate it from the network which is responsible for triggering the black hole attack. The basic idea to detect and isolate milieus node from the network using fake route request packets. In our proposed methodology source node which wants route to destination will flood fake route request packet in the network. The fake route request packets contain the IP address of the node which doesn't exist in the network. The malicious node will reply back to source with the route reply packet. The node which reply with the route reply packet is detected as the malicious node and it is isolated from the network. To isolate malicious node from the network, source again flood the guenon route request packets in the network. The source get various route reply and from the route reply various available paths are there, source never select that path in which the malicious node exist which is been detected in fake route request packets. The proposed technique is implemented in network simulator version 2 and results are analyzed graphically by taking various network parameters like throughput and delay. The proposed technique is implemented in NS2 and simulation results show that this technique is more efficient than the previous techniques. The delay and throughput in the previous and present technique is shown in figure 1 and figure 2 respectively.

a. Proposed Algorithm

Start

1. Deploy mobile ad hoc network with finite number of mobile nodes
2. Source node flood the network with the fake route request packets to detect malicious node
3. If (Any mobile reply with route reply packets)

   {

   That node will be detected as malicious node

   }

   Else

   {

   Source assume that no malicious node exist in the network

   }
4. The source flood the guenon route request packets in the network
5. Source get various route reply packets

   If (Malicious nodes==exists)

   {

   Source will not select the path in which malicious node exists

   }
6. Secure and shortest path is selected between source and destination

   End

V. RESULTS

A. Delay Graph:- In this graph delay is more in new proposed than the existing system. Red lines shows less delay of old system and Green lines shows more delay in new system. This is happened because we are

first searching the malicious node by sending the fake route request packet.

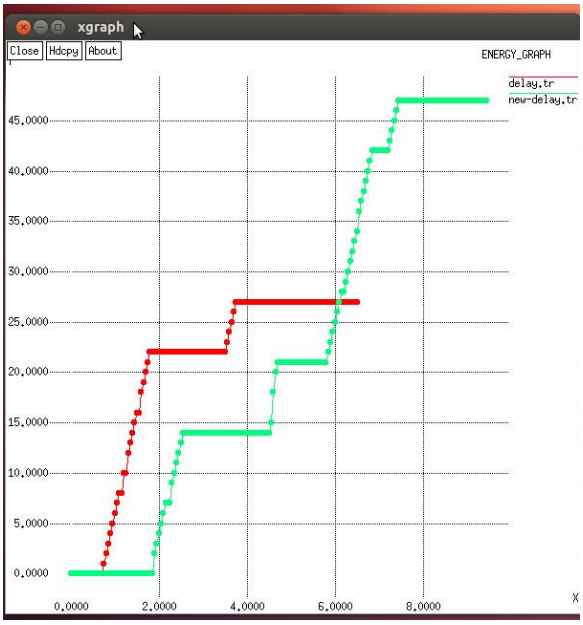

Fig 2: Comparison graph of delay

B. **Throughput Graph:-** As the packet dropped is prevented in this work. So throughput of the proposed system is more than existing system. Red line shows old throughput and green line shows new throughput.

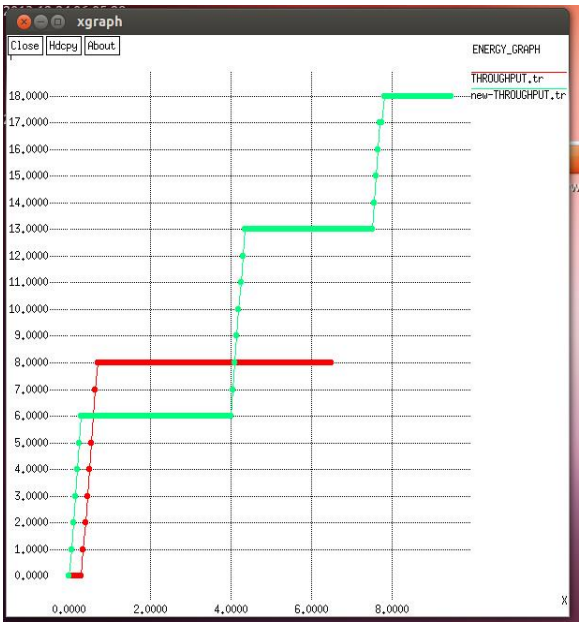

Fig 3: Comparison graph of Throughput

VI. CONCLUSION

In this paper, we conclude that due to the self configuring nature of the mobile ad hoc network much type of inside and outside attacks are possible which degrades the network performance. Among all the security attacks black hole attack is the most common and denial of service attack. In this paper, novel technique is been proposed which is based on the fake route request packets to detect and isolate black hole attack in MANET. The proposed technique is implemented in network simulator version 2 and results are analyzed graphically by taking various network parameters like throughput and delay. The simulation results show that this technique is more efficient than the previous techniques.

In future, the proposed technique can also be applied to detect multiple and cooperative blackhole attack in Manet to increase the performance of the system.

ACKNOWLEDGMENT

I would like to thank ***Er. Birinder Singh***, Coordinator, PTU Regional Center, Baba Banda Singh Bahadur Engineering College, Fatehgarh Sahib for their kind support. I also owe my sincerest gratitude towards Navjot Singh for his valuable advice and healthy criticism throughout my thesis

which helped me immensely to complete my work successfully.

REFERENCES

[1] Hongmei Deng, Wei Li, and Dharma P.Agarwal, "Routing Security in Wireless Ad Hoc Network", IEEE Communications Magazine, Volume 40, Number 10, 2002, pp 70-75.

[2] 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, volume 5, Number 3, 2007, pp 338-346.

[3] Payal N. Raj and PrashantB.Swadas, "DPRAODV: A Dynamic learning system against black hole attack in AODV based MANET", International Journal of Computer Science Issues (IJCSI), Volume 2, Number 3, 2009, pp 54-59.

[4] LathaTamilselvan and V Sankarnarayana, " Prevention of Black Hole Attack in MANET", Journal of Networks, Volume 3, Number 5, 2008, pp 13-20.

[5] Maha Abdelhaq, Sami Serhan, Raed Alsaqour and Rosilah Hassan "A local Intrusion Detection Routing Security over MANET Network", IEEE, July 2011, Bandung, Indonesia

[6] K. Lakshmi et al. "Modified AODV Protocol AgainstBlackhole Attacks in MANET" International Journal of Engineering and Technology Vol.2 (6), 2010, 444-449.

[7] Srinath Perur, Abhilash P. and Sridhar Iyer , "Router Handoff: A Preemptive Route Repair Strategy for AODV" IEEE, 2003

[8] Donatas Sumyla, **"**Mobile Adhoc Networks**",** IEEE Personal Communications Magazine, April 2003, pp. 46-55.

[9] Amandeep Singh Bhatia and Rupinder Kaur Cheema,"Analysing and Implementing the Mobility over MANETS using Random Way Point Model" , International Journal of Computer Applications (0975 – 8887) Volume 68– No.17, April 2013

[10] Jeroen Hoebeke, Ingrid Moerman, Bart Dhoedt and Piet Demeester , " An overview of Mobile Adhoc Networks: Applications and challenges", Sint Pietersnieuwstraat 41, B-9000 Ghent, Belgium ,2005

[11] Dr. A.K Verma , " Mobile Adhoc Networks: An Introduction", 2003

[12] Karthikeyan U and Rajni,"Security Issues Pertaining to Ad-Hoc Networks", 2004

[13] Safa RahimiMovaghar, "Introduction to MANET", Prentice Hall PTR, 2002

Jaspinder Kaur working at CDAC, Mohali, Punjab as Project Tech-II. Qualification is B-TECH in IT branch.

Birinder Singh working at BBSBEC, Fatehgarh Sahib, Punjab as Asst. Professor. Qualification is M-TECH in IT branch.

