International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2019 IJSRCSEIT | Volume 5 | Issue 6 | ISSN : 2456-3307
DOI : https://doi.org/10.32628/CSEIT195655

Black Hole Attack in AODV Based Mobile Ad Hoc Network (MANET)

Khushbu[1], R. K. Bathla[2]
[1]PhD Scholar Madhav Uuniversity Sirohi, Rajasthan, India
[2]Professor, Madhav University Sirohi, Rajasthan, India

ABSTRACT

Mobile ad hoc network (MANET) is a self-configuring network that is formed via wireless links by a collection of mobile nodes without the help of a fixed infrastructure or centralized management. Each mobile node can move freely in any direction, and changes their links to other devices frequently. Security is an essential part of ad hoc networks. Due to its dynamic topology, resource constraints, no centralized infrastructure and limited security, it is vulnerable to various attacks and black hole attack is one of them. In a black hole attack, a malicious node impersonates a destination node by sending a spoofed route reply packet to a source node that initiates a route discovery. By doing this, the malicious node can deprive the traffic from the source node. In order to prevent this kind of attack, it is crucial to detect the abnormality occurs during the attack. In conventional schemes, anomaly detection is achieved by defining the normal state from static training data. However, in mobile ad hoc networks where the network topology dynamically changes, such static training method could not be used efficiently.

Keywords: AODV, Anomaly Detection, Blackhole Attack, MANET

I. INTRODUCTION

Mobile ad hoc network (MANET) is a collection of mobile hosts without the required intervention of any existing infrastructure or centralized access point such as a base station. The applications of MANET range from a one-off meeting network, emergency operations such as disaster recovery to military applications due to their easy deployment. However, due to their inherent characteristics of dynamic topology and lack of centralized management security, MANET is vulnerable to various kinds of attacks. The wired network is used as the backbone of wireless network. When any computer device desires to communicate with other device, all the nodes should lie in between the radio range of each other. The wireless networks are getting popular due its ease of use. Wireless networks are easy to install as compared to the wired network. Based on coverage area, the wireless network can be divided into: Personal Area Network, Local Area Network and Wide Area Network. In the wireless network, the nodes can communicate directly or through a centralized medium such as base station or an access point. Routing is the process of exchanging information from one station to the other stations of the network [3]. It may divide into different aspects. Route construction (topology) based it further divided into three types namely i. Tree based ii. Mesh based and iii. Hybrid. The tree based routing scheme has single path between the source and receiver. In mesh based approach multiple redundant paths connect the source and the destination. The hybrid approach attempt has been made to combine both the mesh-based and the treebased approaches. The first generation of wireless networks started from 1972. At that time, PRNET was

the name given to network system. The ad hoc networks have the history from the DoDi sponsoring PRNET for the armies. The emergence of second generation took place with the enhancement and implementation of ad hoc network as an ally of SURAN program. It has taken the new heights in 1990 with the introduction of notebook computers and the introduction of the mobile of nodes as the brain child at many research platforms. "Ad-hoc networks" was accepted as a term by the IEEE802.11 subcommittee and from then only the versatile regions came under the eye of the researchers and explorers for the implementation of the ad hoc network. Internet Engineering Task Force (IETF), worked hand in gloves with mobile ad-hoc networking groups for the standardization of protocols for routing in ad hoc network.

II. LITERATURE SURVEY

S. Marti et al., (2000) proposed the Watchdog/Pathrater as a solution to the problem of selfish (or "misbehaving") nodes in MANET using DSR protocol. The Watchdog method is used to detect misbehaving nodes and the Pathrater, to respond the intrusion by isolating the selfish node from the network operation. Watchdog runs on each node. When a node forwards a packet, the node's watchdog module verifies that the next node in the path also forwards the packet. The Watchdog does this by listening in promiscuous mode to the next node's transmissions. If the next node does not forward the packet, then it is considered to be misbehaving and is reported. The Path rater module uses the information generated by Watchdog to select a better route to deliver the packets, avoiding the selfish nodes.

Hongmei Deng et al., (2002) proposed the method for detecting the single black hole node in MANET. In this method, the intermediate nodes send RREP message along with the next hop information. After getting this information, the source node sends further request to next hop node to verify that it has the route to the intermediate node or not. If the route exists, the intermediate node is trusted and source node will send data packets via that trusted node. If not, the reply message from intermediate node will be discarded and alarm message is broadcasted and isolate the detected node from network. By using this method, the routing overhead and end to end delay will be increased. If the black hole nodes work as a group in an attempt to drop packets, then this method is not efficient.

Mohammad Al-Shurman et al., (2004) proposed the two methods to avoid the black hole attacks. According to the first solution, the source node verifies the validity of the route by finding more than one route to the destination. It waits for RREP packets to arrive from more than two nodes. When the source node receives RREP packets and the routes to destination have shared hops, the source node can then recognize the safe route. This method causes routing delay. The second solution is to store the last packet sent sequence number and the last packet received sequence number in a table. When node receives reply message from another node it checks the last sent and received sequence number. If there is any mismatch, then the ALARM packet is broadcasted which indicates the existence black hole node. Then the other nodes will come to know the existence of black hole nodes in the network. This mechanism is reliable and faster having less overhead.

Satoshi Kurosawa et al., (2007) proposed the solution based on dynamically conditions of MANET. It uses an anomaly detection scheme. The state of network at each node is expressed by multidimensional feature vector. Each dimension is counted on every time slot. The feature vector includes the number of sent out RREQ messages, number of received RREP messages, the number of received RREP messages, the average of the difference of destination sequence number in each time slot between sequence number of RREP message and the one held in the list. The mean vector is then

calculated and they compare the distance between the mean vector and input data sample. If the distance is greater than some threshold value, then there is an attack. It uses dynamic training method in which the training data updated at regular intervals of time.

III. BLACK HOLE ATTACK

The crucial situations like natural disaster, war footing, business conferences, demands both MANET and the secured communication of data between two nodes. To make this demand a reality, many second routing protocols were developed in the recent past. These proposed protocols prevent the attack on the safety properly and avoid hazardous conditions. Various types of attacks on MANET, like Black hole attack, worm hole attack, denial of service, flooding attack impersonation attack, selfish node misbehaving and many more has made it very challenging and crucial to send the data safely from one node to another. Mobile network security is the need of a day. For this in-depth knowledge of the attacks their behaviours and the damages they may cause must be understood. There are many reasons behind that make MANET prone to these attacks. One of the major reasons is absenteeism of the central point for network management and the communication occurs between the nodes mutually. Vigorously changing topology lack of authentication facility and limited resources add another feather to the cap of attacker. Black hole attack shatters the communication of the route by forging the routing message. This is not the end, further there is drop the packet a forged node and, thus these safety properties get threatened. In Black hole attack the sequence no is forged and forcibly acquiring the route by capturing the hop count of a routing message and make all the data packet drops that passes through it. The malicious node poses itself the destination node by sending the concocted RREP to the source node and start the route discovery. Black hole exhibits to characteristics (1) the node poses itself as destination and having valid route by capturing the node and the ad hoc routing protocol, though the route is fake but this was done to intercept the packets. The malicious node fits in the data route by different methods this has been explained in the figure below: The figure is self-explanatory that node 1 is source node and node 4 is the destination node. When the source node flashes RREQ to find the optimized route to the destination node to the intermediate nodes, the intermediate node continuously receives and broadcast RREQ. Everything works in order if the RREP from the normal destination node reaches the source node. As shown the node 3 is an attacker node and act as black hole. Now the node 3 send RREP from itself to the source node before any other intermediate node send the same, making the source node assume that route discovery process has been complete and starts sending the data packets. In the black hole attack the malicious node send RREP to the source node with the hope count of 1 and having large sequence number, in this way the source node will select the malicious node as the destination node as it exhibits minimum hop count after receiving the RREQ from the source node and start sending the data packets to malicious node considering it as the destination node. The Black has got one property that it does not forward any packet and makes all the packets get dropped to itself without the knowledge of source node. The Source node assumes the packets are moving to the destination without having any information that the route has been attacked and the packets are not received by the actual destination node. If these kinds of nodes are multiple in nature and present in a single MANET, makes a situation a crucial, complex and hazards.

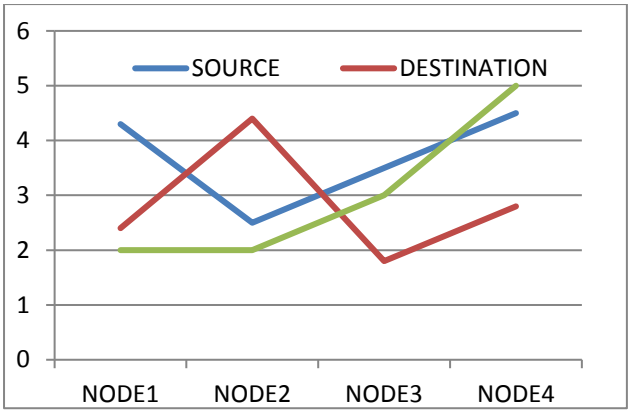
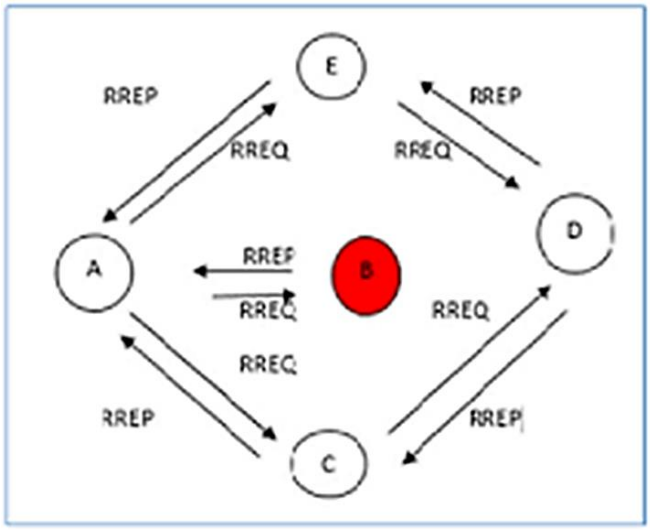


Fig 1.1



CHARACTERISTICS OF MANET

a) Communication via wireless medium.

b) Nodes can perform both the roles of hosts and routers.

c) Dynamic network topology. Frequent Routing Updates.

d) Can be set up anywhere.

e) Autonomous.

f) Lack of centralized administration.

g) Energy Constraints.

h) Limited Security.

i) Limited Bandwidth

APPLICATIONS OF AD HOC NETWORKS

Due to cost-effectiveness of MANET, it is being used in vast application areas that includes military applications, rescue operations, wireless sensor networks, etc. These applications are described as

1. Military applications: As the ad hoc networks can be established or deployed quickly, it can be beneficial for providing quick communication between soldiers in the battlefield. There should be secure communication between the soldiers as it required privacy. The long life batteries should be equipped in nodes for long term communication.

2. Emergency operations: With the self-organization of the ad hoc network; there is minimal overhead to deploy it. Due to natural calamities like earthquakes, it is difficult to establish the fixed infrastructure wireless network quickly; the ad hoc network could be deployed immediately for the coordination in rescue operations. There should be minimum delay during communication in ad hoc network.

3. Commercial Sector: The ad hoc network is extensively used in collaborative and distributed computing applications. For the communication between groups of people in a business-oriented conference, it will be efficient to establish ad hoc network instead of centralized network. The ad hoc network can be used in distributed file sharing applications also. It can be used in mobile offices, dynamic database access and also in electronic payments.

4. Education & Entertainment Sector: With the ad hoc networks, the interactive education can be provided by establishing the virtual classrooms in the schools and colleges. The ad hoc based network in a University or campus provides communication between students and teachers during the lectures and meetings as well. The ad hoc networks are also used for entertainment

purposes like in multi user games, robotic pets, theme parks, outdoor internet access etc.

5. Wireless Sensor network: Wireless sensor network is a collection of spatially distributed autonomous sensors which works cooperatively to monitor the environmental or physical conditions like temperature, humidity, sound, pressure etc and pass their data to the main location. The application areas of sensor networks are environment monitoring, health care, home security, health care etc. The technical issues like mobility of nodes, size of network, power constraints, density of deployment and traffic distribution are need to be considered during its deployment.

IV.CONCLUSION

After completion study of publish paper the result will be like this. The throughput of proposed work is more as compared to previous work that means the delivery of data packets are successful. Packet Delivery ratio is better comparing to previous. As shown in fig.1.1. when we want maximum throughput, more delivery ratio and less delay then we will use this modified TAODV. We find this following conclusion after using this proposed TAODV.

V. REFERENCES

[1]. Jaspal Kumar, M. Kulkarni, Daya Gupta), "Effect of Black Hole Attack on MANET Routing Protocols", IJCNIS, 5, (2013), 64-72

[2]. Sowmya K.S, Rakesh T. And Deepthi P Hudedagaddi (2012), "Detection and Prevention of Blackhole Attack in MANET Using ACO", International Journal of Computer Science & Network Security, May2012, Vol. 12 Issue 5, p21-24. 4p

[3]. Rajni Tripathi And Shraddha Tripathi , "Preventive Aspect Of Black Hole Attack In Mobile Ad Hoc Network", IJAET, (2012) ISSN: 2231-1963

[4]. Tanu Preet Singh Neha Vikrant Das (2012), "Multicast Routing Protocols in MANETS", Volume 2, IJARCSSE(2012)

[5]. Ram Ramanathan and Jason Redi, "A Brief Overview of Ad hoc Networks: Challenges and Directions," IEEE Computer Magazine, pp.20-22, 2002.

[6]. Sheltami, Tarek, "Ad hoc Network Overview," http://www.ccse.kfupm.edu.sa/~tarek, Ad hoc network Technology, 2003.

[7]. Changling Liu and Jorg Kaiser, "A Survey of Mobile Ad hoc Network Routing Protocols," Univ. of Ulm, Tech. Rep.Series, 2005.

[8]. Krishna Gorantala, "Routing Protocols in Mobile Ad hoc Networks," Master Thesis in Computing Science, Umea University, Sweden, 2006.

Cite this article as :

Khushbu, R. K. Bathla, "Black Hole Attack in AODV Based Mobile Ad Hoc Network (MANET)", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 5 Issue 6, pp. 346-350, November-December 2019. Available at doi : https://doi.org/10.32628/CSEIT195655
Journal URL : http://ijsrcseit.com/CSEIT195655