A SURVEY ON PREVENTION OF BLACK HOLE ATTACK INMANET

Hina Rabbani[1], Shailja Nema[2]

[1]*M.Tech Department of Computer Science & Engineering, Babu Banarasi Das University, Lucknow, India*
[2]*Department of Computer Science & Engineering, Babu BanarasiDas University, Lucknow, India*

Abstract

The Mobile Ad Network is a collection of mobile nodes that can communicate with each other via wireless links without using fixed infrastructure or centralized infrastructure. Since there is no centralized infrastructure each node acts as a router as well as hosts. Manets often suffers from security breaches because of its characteristics like dynamic topology, self-configuring node etc. These types of network may be within the network or outside the network.Black hole attack is one of them. Black Hole attack is a type of attack where a node starts behaving selfishly or starts misbehaving in terms of packets. Manets adopt AODV (Ad Hoc on Demand Distance vector) routing protocol. One of the major issues in AODV is Black Hole Attack. The malicious node advertises itself as the shortest path to the destination and the source sends the data to the malicious node and then all the packets are dropped out by the malicious node. This paper provides a comprehensive research on prevention of black hole attack in Manet. A wide variety of literature in this field had been identified and reviewed.

Keywords:-*Manet, Black hole,AODV*

----------***----------

1. INTRODUCTION

In the ever increasing demand of wireless technology, Manet is widely in acceptance. A Manet is a group of nodes or communication devices that can communicate with each other without any fixes infrastructure. Nodes may be laptops, mobile devices, pda's, etc. Manet communicate with radio link and the node that are within the radio range can communicate directly but the nodes that are out of radio range uses intermediate nodes to route the information from source to destination.

One of the most important characteristics of Manet is dynamic topology and its self-configuring nature. Any node can join or leave the network at any time, thus the network topology may change dynamically and at unpredictable times. Manet are also self-configuring since there is no central hub hence, starting from the discovery of topology till the delivery of messages is done by the nodes themselves.

Due to its unique characteristics, Manets are more prone to attack. Asmentioned earlier that any node can enter or leave the network so any type of intruders can attack the communication at any time, especially during routing. Nodes within the Manet communicate on the basis of mutual trust. This mutual trust makes Manet more vulnerable to attack inside the network. Malicious nodes or selfishnodes are the ones that emerge by taking advantage of mutual trust and these selfish nodes led to various security attacks like Black Hole attack or Gray Hole Attack.

Network Security is one of the most important and challenging task and to have a secure communication we must be aware of various types of attacks and their effects. Different types of attack in Manets are Black Hole attack, Sybil Attack, Rushing Attack, Grey Hole attack, Sinkhole Attack etc. These attacks mainly come during routing in nodes. Different routing protocols used in Manets are Proactive routing(DSDV), Reactive Routing (AODV) and hybrid routing (ZSR). Manet are widely used for military operations, emergency operations etc.

2. AODV (Ad-Hoc ON DEMAND DISTANCE VECTOR) ROUTING PROTOCOL

Frequent used routing protocol in Manet is AODV.AODV is a reactive routing protocol. Since it is on demand routing protocol there is no need to maintain routing table or information at the nodes when there is no communication. Advantage of this protocol is that wasted bandwidth gets reduced. Disadvantage of this protocol is that it leads to packet loss. AODV creates routes between two nodes only when needed. When a node wishes to start the communication with another node in the network and if there is no route, AODV will provide the route. It uses sequence number and hop counts to check whether routing information is up to date. Routes are maintained as long as they are needed by the source. AODV uses three control messages to find the route from source to destination.

1. **Route Request Message(RREQ):**
   Whenever a node wants to communicate with another node in the network, it transmits RREQ messages. AODV broadcasts RREQ messages in the network usingexpanding ring technique. Every RREQ message has a TTL (Time to Live).

2. **RREP(Route Reply Messages):-**
   A node having received RREQ generates a route reply RREP message back to the source from where RREQ was generated.

3. **RRER(Route Error messages):-**
   If a node detects a link crack in an active node, RRER is generated.

Mechanism in AODV

In AODV, the node that wants to start the communication will broadcast the RREQ. Every node will perform either of the two functions:-

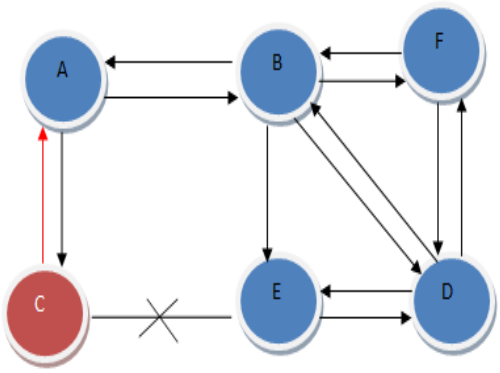
- If a node has route to the destination it will send RREP message to the sender.
- If it has no route to the destination it will make entry in routing table regarding the sender node, increment the hop count within RREQ message

Now, when the route request reaches the destination, it reverses the path and replies RREP message to the sender. The source will send the packets to the earliest RREP message which it has received. And later on, the RREP messages which it has received will be discarded.

If a link break occurs, the node sends an RRER (route error) message to the sender and the route discovery is regenerated is still needed by the sender.

3. BLACK HOLE ATTACK

Manet attacks are categorized in two main categories. Active and Passive attack. Black Hole Attack is a type of active attack. These attacks have malicious node and this malicious node claims to have the shortest path to the destination. Whenever it receives RREQpackets, it sends RREP with highest sequence number and minimum hop count value. So, the source delivers the packet to the malicious node and malicious discards all the packets.



Suppose node A, wants to send data packets to destination D, it will broadcast RREQ message to the network and the malicious node C also receives RREQ. So, it will send RREP message with highest sequence number and minimum hop count value. Node A will get the RREP message and will discard all the other responses and will start sending the packets to the malicious node C. Malicious node C after receiving the data packets will discard all the packets and will not forward the data packets.

4. RELATED WORK

In this section we will study about various techniques used in prevention of black hole attack by different authors. Various prevention techniques have been proposed and a brief study of these techniques is mentioned here.

[1] Latha tamilselvan and Dr. V. Sankaranarayan proposed a method which was an enhancement of basic AODV routing protocol. A protocol called SAODV had been used in which waiting concept is used. The sender waits for all the RREP and checks if any of the nodes have similar hop count value. If it finds a similar hop count value for two intermediate nodes it will send the packets with that path else will have to send with the malicious path. It maintains two tables. One is Timer expired Table for collecting further request from various node. The other node Collect Route Reply Table to store the sequence number and the time at which packet arrives. A feasible solution is prepared to avoid black hole and network simulator GLOMOSIM is used.

[2] Adnan Nadeem and Michael Howarth proposed a generalized from of prevention from all types of attacks. Two techniques are used i.e. knowledge based intrusion detection (KBID) and the other is Anamoly Based Intrusion Detection (ABID). KBID detects attacks whose signature is already present in the database while ABID provides early warning. Generalized Intrusion Detection and prevention (GIDP) technique is used which have cluster heads (CH) and cluster nodes (CN).Cluster gather information in two matrices NCM(Network Characteristic Matrices) and DM (derived Matrices). A new Knowledge base is prepared for the suspected attack and their signatures are stored in the database for further prevention of attacks.

[3] Jian Ming Chary and Po-Chun Trou presented a mechanism for Black Hole attack known as cooperative Bait Detection Scheme. With the help of CBDS, the address of adjacent node as the bait destination address, it baits malicious nodes to reply RRCP and detects the malicious node by the reverse tracing program. Whenever there is significant drop in packet delivery ratio, an alarm will be sent by the destination node to the source to trigger the detection method. Consequent much of the data packets loss can be overcome, and present good performance in terms of better packet delivery ratio.

[4] Kamarularifin Abd Jalil et.al presented an enhanced protocol of AODV called ERDA, which is used to prevent Black Hole Attack problem. Few more tables are added to the AODV routing table to keeptrack of all nodes and its corresponding sequence no. Source has all the record. Now source node analyses the sequence no. by heuristic and captures the malicious node which has highest sequence number.

[5] Deng proposed a novel approach for detection of black hole. In this method information about the next hop to the destination should be included in RREP when any intermediate node replies for RREP. Now, source node will send a further request to the next hop of replies node and asks about the replied node and its route to the destination. We can check the trustworthiness of the replied node only if the next hop is true. But it prevents attack only for single black hole .Cooperative black hole attack is still pursuing.

[6] Pramod Kumar Singh and Govind Sharma proposed a simple and efficient prevention of Black Hole Problem. Firstly,source send RREQ message and after having received the RREP message it finds the route of the destination. Now it will simply send a HELLO message and if it reach thedestination it will send an acknowledgement that it has received the HELLO message.So, it will be sured that it is not a malicious node. But the overall performance is reduced Network Simulation is used .Qual Net 5.0.1 network simulation tool is used.

[7] Jitendra Saoner and Vinit Gupta developed an approach for Black Hole Prevent by forming duster. All the devices are categorized into 3 levels like mobile node, cluster heads and a monitoring server.Whole sole responsible is with the server to calculate the trust value for securing the network from attack. All types of trust are check either if the communication is between internal clusters or between external clusters or between unknown nodes if any of the nodes is suspected it will be declared as malicious node.

5. CONCLUSION AND FUTURE FRAMEWORK

This paper reviewed various mechanisms to prevent black hole attacks in Manet. Since, black hole attack occurs in AODV protocol. Hence, our main focus was on AODV protocol. Various researches have been made and enhance form of AODV protocols are made like SAODV etc. However, the consequent of black hole attack have been overcome to a much extent but various parameters like network throughput, end to end delay needs to be more effective because implementation of these enhanced protocol have reduced the capability of above said parameters.

REFERENCES

[1]. Latha Tamilselvan Dr. V Sankaranarayan “Prevention of Black hole Attack in MANET” The 2nd International Conference on Wireless Broadband and Ultra Wideband Communications (AusWireless 2007) 0-7695-2842-2/07, IEEE 2007

[2]. Adnan Nadeem Michael Howarth “A Generalized Intrusion Detection & Prevention Mechanism for Securing MANETs” 9781-4244-3941-6/09 2009 IEEE

[3]. Jian-Ming Chang Po-Chun Tsou Han-Chieh Chao Jiann-Liang Chen “A Cooperative Bait Detection Scheme to Prevent Malicious Node for MANET Based on Hybrid Defense Architecture” 978-1-4577-0787-2/11 IEEE 2011

[4]. Kamarularifin Abd Jalil, Zaid Ahmad, Jamalul-Lail Ab Manan ," Securing Routing Table Update in AODV Routing Protocol", 2011 IEEE Conference on Open Systems (ICOS2011)

[5]. Hongmei Deng, Wei Li, and Dharma P. Agrawal, “Routing Security in Wireless Ad Hoc Network,” IEEE Communications Magazines, vol. 40, no. 10, October 2002.

[6]. Pramod Kumar Singh Govind Sharma “An Efficient Prevention of Black Hole Problem in AODV Routing Protocol in MANET”11th International Conference on Trust, Security and Privacy in Computing and Communications 978-0-7695-4745-9/12 IEEE 2012

[7]. Jitendra Sayner Vinit Gupta “Clustering of Mobile Ad Hoc Networks: An Approach for Black Hole Prevention” 978-1-4799-2900-9/14/$31.00 ©2014 IEEE