PREVENTION FOR BLACK HOLE ATTACK USING HONEY-POT TECHNIQUE IN AODV PROTOCOL

(*Huma Tariq*), (*Sidra Anwar*)

(Huma Tariq) Department of Computer Science, Government College Women University, Sialkot, Pakistan; (Sidra Anwar) Department of Computer Science, Government College Women University, Sialkot, Pakistan.
Email: (humatariq773@gmail.com, sidra.anwar@gcwus.edu.pk)

ABSTRACT

Mobile ad-hoc network is a kind of network which is infrastructure-less and can be designed for fulfilling particular purpose that is served by the establishment of the whole setup on the fly. In this research, we have analysed the detection of black hole attack with prevention solution to black hole attacks on AODV protocol. As mobile nodes send data packets using intermediate nodes and due to week security mechanism, MANET suffers from many intruders attacks. Black Hole attack is a denial of service attack and when a malicious node sends RREP to source node to show its fresh and shortest path to destination and after receiving data packets, drop them or share with another malicious node instead of uncompromised forwarding to destination node. In this study, an approach is proposed for the detection and prevention of black hole attack and making the path secure from malicious node involvement by using Honey-Pot technique and keeping secure the network by broadcasting malicious node address to other nodes in network.

Keywords: AODV, MANET, Black Hole Attack, Honey-Pot, Fox node, Replica packet, trap table. RREQ (Rout Request), RREP (Rout Reply).

1. INTRODUCTION

Cloud networks are very broad but unreliable because of its elastic nature. Due to this nature, nodes can join and leave the network at any time [10]. In the world of computing, security is a major concern.MANET is extensively used in armed purpose [11], tragedy era and personal system .We discus Black hole attack on Mobile Ad hoc network in Ad-hoc on demand distance vector (AODV) protocol.

1.1 MANET

Since the emergence of set of new networking approaches and challenges even for the fundamentals of routing, the mobile ad hoc networks (MANET) are found significantly different from the wired networks. Mobile Ad hoc Network is a type of network which is self-configured in its own infrastructure [3] having autonomous nodes to form a multi-hop network for communication. The transmission of mobile hosts is received by all hosts within its transmission range due to the broadcast nature, communication and omnidirectional antenna.The transmission of data packets between two wireless hosts can be transferred by other mobile hosts located between them [5] and can forward their messages, which effectively build connected network among mobile hosts in the deployed area. Each node in MANET acts both as router and as a host [9]. Several routing protocols have been designed for MANET to optimize network routing performance.

1.1.2 BLACK HOLE ATTACK

The scope of this paper is to analyse the effect of black hole in MANET on the performance of Reactive routing protocol i.e. ad hoc on Demand Distance Vector (AODV). Comparative analysis of black hole attack for this protocol is taken into account. The impact of black hole attack on the performance of MANET is evaluated finding out is this protocol is more vulnerable to the attack and how much is the impact of the attack on this protocol. The measurement taken in the light of throughput, number of packets drop and packet delivered ratio. A malicious node observed to use routing protocol to advertise itself [7] as having the shortest path to the node whose packets it wants to intercept. This malicious node then can choose whether to drop the packets to perform a denial-of-service attack [1].

1.1.3 AODV PROTOCOL UNDER BLACK HOLE ATTACK

AODV is a reactive routing protocol .It uses a destination sequence number to ensure freshness of route and guarantee loop freedom [5]. When a node needs to send data packets to destination, first it check its routing table for existing routing, if no route is found then it initiates a RREQ (Route Request) request [6] and broadcast this request to all the neighbors to find a fresh and shortest route to a desire destination. This process is called route discovery. The neighbors update their table according to the RREQ request. If path is not available, it will increment the hop count by one and further broadcast a RREQ [3]. During the transmission of data if any node identifies route break, it will send a RERR (Rout Error) message.

Fresher path is measured by its destination sequence number. Source node choose path with a higher destination sequence number and low hope count. In the black hole attack malicious node receive route request packet and send RREP with a higher destination sequence number as shown in Fig.1. Source node see the RREP with a big sequence number and consider that the route is fresh and start sending data packets. The malicious node does not forward the data packet and drop them, [7] thus reduce packet delivery ratio and increase network congestion. In Fig.1 source node is S and D is destination node and malicious Node sends a forged RREP to source node S with a high sequence number. As source node do not have any prior information about destination in this table. It starts sending data to node M which instead of sending data packet to C for further data transmission, drops all data packets or sends them to other malicious node.

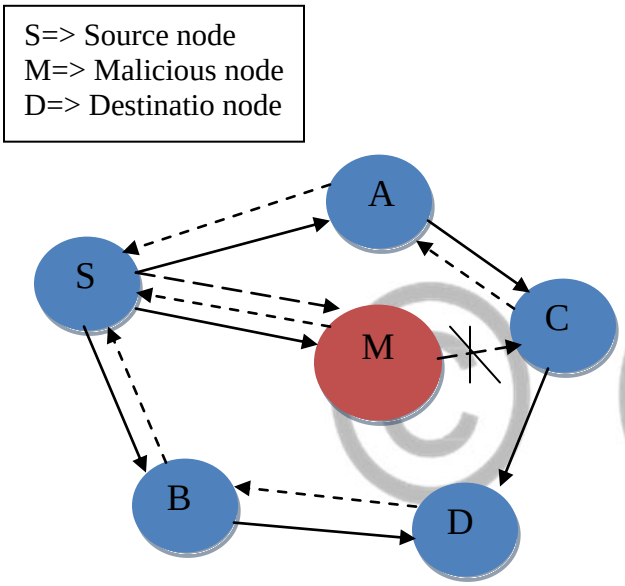
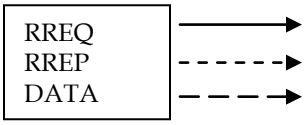


Fig.1: Black Hole Attack

Fig.1 shows black hole attack on data packets.It is a good representation of black holeattack.In this Fig, source node considers malicious node and drop packets instead of sending it to C.



2. Literature Survey

2.1 SAODV (Solution of Black Hole attack)

Latha Tmil Selvan and Dr. V Shankar Narayan has proposed a solution [7] in which source node instead of sending data packet to a node reply at once will wait and check the reply from other neighboring nodes until times out. All the replies from neighbor nodes are collected in CRRT (Collect Rout Reply Table) [3]. It then checks in CRRT whether there is any repeated next hope node. If a repeated next hope node is located it is assumed that the reply path is safe and probability of having Black hole attack is limited.

2.2 Comparing destination sequence number

Pooja Jaiswal and Dr. Rakesh Kumar [9] have proposed a method to prevent Black hole attack in AODV. In the method source node collects all the RREP from different intermediate nodes. The first entry received by node is marked first entry in Rout reply table (RRT). The destination sequence number (DSN of first entry) is compared with sequence number of source node. If the DSN of the first entry is very large as compared to source sequence number, the node is considered as malicious node and removed from the RRT [3]. Path is selected based on remaining entries in RRTE which is arranged according to DSN. The node with highest DSN is selected for path.

3. Proposed Prevention Technique

In this research, an improved technique has been proposed for the prevention from black hole attack in AODV protocol. It is proposed that, for making data transactions in a secure manner, we transform our simple source nodes into FOX source node (sharp node), using Honey-Pot technique inspired by a computer based system Distributed Intrusion Detection (Honey-Pot technique).When a node needs to send data packet to destination, it broadcasts a RREQ(Rout Request) to all its neighbors to find a shortest path, when neighbor node sends RREP (Rout Reply) to source node, then source node which is intelligently transformed into FOX source node (sharp node) instead of sending data packets to neighbor nodes it will generate a Replica packet which represent itself as data packet but, it never contains data and only use for keeping track of that neighbor node's activity. This Replica packet looks like a data packet and used to attract the hackers or malicious nodes; the source node contains a counter called trap count. When the Replica packet sends to other node by neighbor node according to hope-count number, the Replica packet go back to FOX, source node's trap counter will be incremented by 1.Source node consider that neighbor node are safe nodes and sends original data packet to that neighbor node.

If Replica packet does not go back to source node then, it will be considered that the neighbor node does not send that Replica packet to further to another neighbor node then trap counter cannot be incremented, so source node considers that black hole attack occured and Replica packet may be sent to another malicious node or dropped. That node considered as a malicious node by source node saves the address of that malicious node in its routing table and broadcast this address to all its neighbors. In this way, all neighbor nodes also identify that malicious node more easily and never send any data packet to it. After receiving RREP reply from a node, source node match its address information with routing table data if it is not matched it will be entertained, otherwise source node update its address information, broadcast it to all neighbors and ignore its request.

3.1 HONEY-POT Technique Pseudo code

1. FOX source node broadcast RREQ (Rout Request) to all neighbours for finding shortest and fresh path.
2. Neighbour nodes send RREP (Rout Reply) for data packet.

3. FOX source node sends Replica packet to that neighbour node using Honey-Pot technique, neighbour nodes considered that Replica packet as data packet.

4. If Replica sends to other neighbour node then it will be tracked by FOX source node and FOX source node considered that path safe for data delivery and sends original data packet to that neighbour node and trap counter of FOX source node will be incremented by 1.

5. If Replica packet does not go back to FOX source node then it will considered as a malicious attack and FOX source node saves that malicious node information and broadcast that information to all its neighbours.

6. All neighbour nodes save that information and always ignore the RREP from malicious node.

7. Using this Honey-Pot technique and transformation of simple source nodes into FOX source node, is a better way to make data packets secure from Black Hole attack.

4. Results and Discussion

Under the research of black hole attack analysis and prevention technique, there is an observed alarming situation of data leakage [11]. Many solutions had been provided but still suffering from this problem. There is needed to make a strong security mechanism among nodes and establishment for identification of safe and secure node before transmission. For the prevention of black hole attack on data packets, we proposed Honey-Pot technique to make better identification of malicious node. In this research after analyzing this serious data packet dropping threat, we transform source node into sharp node and these sharp nodes are called FOX source node. For the transformation of secure node, we introduced Honey-Pot technique. In this technique, we proposed a Replica of FOX source node (Transformed source node also called sharp node) data packet and broadcasted this Replica to neighbors, if this Replica returns back to FOX source node then that neighbor node would be considered as secure node.

5. Conclusion and Future Scope

The research introduced a new concept of prevention from black hole attack. We introduce a Honey Pot technique which is used in network intrusion detection system (IDS). Using this technique, we can transform our simple source node into FOX node, also called sharp node. After receiving RREP from neighbor node as freshest path to destination node, instead of sending a data packet to that neighbor node, Fox node sends a Replica packet to that neighbor which sends RREP to it. This Replica represents itself as Data packet and attracts hackers or intruder node in this way that intruder considers it as data packet and performs its malicious activity. This Replica saves its necessary information and sends it to Fox node and Fox node broadcast this information and make Data transmission secure from Black hole attack. There are many solutions are introduced by many researchers with reliability issues because most of the procedures having more time delays. There is need to work on the improvement of time delays on data packet delivery, and data security as well.

References

[1] Kamaljit Kaur, Gaurav Raj, "Comparative Analysis of Black Hole Attack over Cloud Network using AODV and DSDV K", IEEE 2015.

[2] Umashkar Ghungar, Dr.Jayaram pardhan ,"A Study on Black Hole Attack in Wireless Sensor Networks" 2017.

[3] Sakshi Jain, Review of Prevention and Detection Methods of Black Hole Attack in AODV- based on Mobile Ad Hoc Network, International Journal of Scientific and Research Publications, Volume 2, Issue 9, September 2012.

[4] Arshdeep kaur, Mandeep kaur," A SURVEY BLACK HOLE ATTACK IN MANET", International Journal of Science, Engineering and Technology Research (IJSETR), Volume 4, Issue 5, May 2015.

[5] Ms Monika Y.Dangore , Mr Santosh S. Sambare,'Detecting And Overcoming Blackhole Attack In Aodv Protocol'2013.

[6] Mohamed A. Abdelshafy, Peter J.B. King, "Resisting Blackhole Attacks on MANETs"2016.

[7] Latha Tamilselvan and Dr. V Sankaranarayanan, "Prevention of Blackhole attack in MANET", BSA Crescent Engineering college, 2007 IEEE.

[8] Durgesh Kshirsagar and Ashwini Patil, "Blackhole attack prevention and detection by real time monitoring", 4th ICCCNT 2013.

[9] Pooja Jaiswal and Dr. Rakesh Kumar "Prevention of Blackhole attack in
MANET", IRACST, October 2012.

[10] Bilel Zaghdoudi, Hella Kaffel-Ben Ayed, Imen Riabi, Ad Hoc Cloud as Service:A Protocol for setting up an Ad hoc Cloud over MANETs, The international workshop on networking algorithms and technologies for IoT (NAT-IoT) 2015.

[11] Arshdeep kaur1, Mandeep kaur ,"A SURVEY BLACK HOLE ATTACK MANET", Issue 5, May 2015.