A Review Study on Preventing and Detecting Technique of Black Hole Attack in MANET

Kavita Babriya
M.Tech Scholar, Department of Computer Science & Engineering OITM Juglan Hisar (Haryana)

Surender Singh
Asst. Professor, Department of Computer Science & Engineering OITM Juglan Hisar (Haryana)

ABSTRACT

There are basically two types of black hole attack i.e. internal black hole and External black hole attack. Black hole is a malicious node that wrongly replies for some route requests without having active route to particular destination and drop all the getting packets. If these malicious nodes work jointly as a collection then the damage will be very risky. This type of attack is called cooperative black hole attack. Black hole attack is a type of active attack. Black hole attack can arise when the malicious node on the path attack the data transfer and purposely drop, delay or change the data transfer passing through it. Black hole node treats itself as a trusted node. This is review study on Black hole node send false routing information, claim that it has a best route and cause additional good nodes to route data packets through the black hole node.

Keywords: MANET, AODV, BLACK hole attack, MN-ID

I. Introduction

With the fast growth of wireless method and expansion of computers, mobile computing has already become the field of computer communication in highly manner that include cell phones, laptop, handheld device [30]. Mobile ad hoc network is completely a wireless network that is very popular now days. Basically there are three types of wireless network that is ad hoc network, infrastructure network and hybrid network which is a combination of both networks [1]. An infrastructure network consists of wireless mobile device and one or more bridge, which attach the wireless network to the wired network. These bridges are called base stations. A mobile node within the network searches for the nearest base station (e.g. the one with the best signal strength), connects to it and communicates by it. The main fact is that all communication is taking place among the wireless node and the base station but not among dissimilar wireless nodes. While the mobile node is traveling around and all of a sudden gets out of range of the current base station, a handover to a new base station will let the mobile node communicate flawlessly with the new base station [3]. Infrastructure network is also called infrastructure basic service set. In this, we can communicate in two pass, in first pass frame are sent to access point and in second pass frame are sent from access point to target node.

A mobile ad hoc network is a self-adjusting and dynamic network in which two or more nodes that can communicate with each other directly [8]. All the nodes leave or join the network anytime and anywhere without help of central control in the network [8]. Every node in an ad hoc network must be prepared to forward packets for other nodes. Thus, every node acts both as a router [11]. Each node finds a path to transfer the data using routing protocols [11]. The dynamic nature of MANET allows nodes to join or leave at any time that increase the chances of attack [7]. This network is decentralized in which nodes are adjusting everything like message delivery and network organization [9]. MANET is open medium network in which chances of attack is very high [7]. Some attack drops the packets in the network and some are modify the packets [9]. There are different characteristics which is a challenge in MANET include bandwidth issue, dynamic topology, restriction on the size of device [5].

In MANET, There are various protocol like reactive, proactive and hybrid protocols. We are supporting the AODV (ad hoc on demand distance vector routing protocol). In this black hole attack is very harmful attack which drops the network packets and affect the network performance. Black hole is a malicious node

that wrongly replies for some route requests (RREQ) without having active route to particular destination and drop all the getting packets. If these malicious nodes work jointly as a collection then the damage will be very risky. This type of attack is called cooperative black hole attack. Various factors affect the network performance:

- Security Threats: In MANET, chances of attack are very high because of this open medium and infrastructure less feature [10].
- Limited Bandwidth: mobile ad hoc network have less capacity than infrastructure network and in this chances of noise, interference is very high because of this bandwidth is very high.

II. LITERATURE SURVEY

In this we present an overview of earlier work related to mobile ad hoc network. Literature survey is the collection of available document on the topic which contains information, ideas, data and evidence written from a particular standpoint to accomplish certain aim or express certain views on the nature of the topic.
Khin and Phyu.T (2014) discuss the impact of Black hole attack on AODV Routing Protocol. In this paper, we are simulating and analyze the impact of black hole attack on Ad Hoc On-Demand Distance Vector (AODV) protocol. The simulation is done by NS-2 and the simulation results are analyzed on various network performance metrics such as packet delivery ratio, normalized routing overhead and average end-to-end delay [12]. The simulation results illustrate that when the black hole node exist in the network, it can be affect and decrease the performance of AODV routing protocol. [7].

Sharma.R and Shrivastava.R (2014) introduced a modified AODV routing protocol to prevent from Black hole attack in Mobile ad hoc network. A Mobile ad-hoc network is a short-term network set up by wireless nodes moving random in the spaces that have no network infrastructure. Mobile ad-hoc networks are unguarded to attacks of the malicious nodes. One of these attacks is the Black Hole Attack against network integrity absorbing all data packets in the network. In this research paper we change the working of AODV routing protocol to stop black hole attack. So we inspect the performance impact of a black hole attack on a mobile ad hoc network and compare it with our modified AODV routing protocol. The simulation work is carried out by OPNET Modeler. To analyze performance of our proposed algorithm we use Network throughput, network weight, packet send and received, packet dropped and end-to-end delay. The consequences of this algorithm are that it only prevents single node black hole, co-operative black hole attack cannot be prevented. The routing overhead also increases because of two further control messages [8].

Kaur.R and Karla.J (2014) discuss the Prevention and detection of Black hole attack in MANET. A mobile ad hoc network (MANET) is infrastructure less dynamic network consist of a group of mobile nodes that talk with each other without the use of any central authority. Security in MANET is the most important concern for the network. The dynamic topology of MANETs allows nodes to connect and leave network at any point. Security of AODV protocol is compromise by a particular type of attack called black hole attack. A malicious node advertises itself as having the shortest path to the node whose packets it want to interrupt. In this paper we are trying to find the secure path for communication through Digital Signature[r 6]. A future scope of this is to find a helpful solution to the black hole attack on AODV [7].

Pooja and Kumar.V (2014) discuss the detection of Black hole attack Technique in MANET. Mobile Ad-Hoc Networks (MANET) is top area of research which is dynamic, self- adjusting and self-organized network. In MANET, nodes are not physical connected to each other, but the communication can takes place if nodes are in range with each other. Because of mobile nature of nodes, the topology of MANET changes from time to time and they lack fixed infrastructure, due to which MANET is open to many security attacks. In this paper, the author discusses Black hole Attack, which is one of the serious attacks in MANET and evaluation of various Black hole Attack finding techniques. Some authors modified the existing protocols and some planned their new protocols [12].

Sharma A and Deshmukh.M (2014) implement the security in Wireless network for Black hole attack avoidance. Wireless networks are computer networks that are not associated by cable of any type. They had some flaw also which were overcome by the future

system. Proposed system helps us in protecting against the black hole attack without any condition of hardware and special detection node [2]. Funde.N and Pardhi.P.R (2013) introduce Detection and Prevention Technique to Black hole and Gray hole attack In MANET. Mobile ad hoc network (MANET) is a self-configuring network of mobile nodes created anytime and anywhere without the help of a permanent infrastructure. It has much possible application in disaster relief operations, military network, and commercial environments. Due to open, dynamic, infrastructure-less nature and self-adjusting, the ad hoc networks are vulnerable to various attacks. AODV is an important on-demand distance vector routing protocol for mobile ad hoc networks. It is more vulnerable to black & gray hole attack. In MANET, black hole is an attack in which a node shows malicious performance by claim fake RREP message to the source node and equally malicious node drops the entire receiving packet. In this paper, we have review different techniques to prevent black & gray hole attacks in MANET. [8].

III. AODV Routing Protocol and Black hole attack

AODV is an ad hoc on demand distance vector routing protocol that is work on the basis of demand of route when it is required by the source node to the destination node [1].AODV is improvement over Destination Sequence Distance Vector (DSDV) protocol. DSDV creating the small ad hoc network [11]. It requires universal distribution of connectivity information for right operation; it leads to frequent system-wide broadcast. so the size of DSDV ad-hoc networks is strongly restricted. When using DSDV, every mobile node also wants to maintain a whole list of routes for every destination within the mobile network. The benefit of AODV is that it tries to reduce the number of required broadcasts. It creates the route on an on-demand basis, as oppose to maintain a complete list of routes for each destination [11]. AODV does not maintain a routing table. When a node wants to communicate with another node, firstly a node sent a route request (RREQ) to the entire node in the network. All the middle node check whether it is the target node or it has a fresh route to go to the target node. If it is vacant, the middle node sends back Route Reply message (RREP) to the source node. Otherwise, it forwards the RREQ message to its neighbors by using flood approach. This procedure is continuous until whether the destination node is found or the node that has a fresh enough route to the destination is found. Once finishing the route discovery process, the source node and the target node can be communicate and send the packets between them. When any node knows a link break or crash, Route Error (RERR) note is send to all other nodes [6]. Hello message is used for detecting and monitoring links to neighbors. Because of route error chances of attack is very high. Here we discuss the AODV Routing Protocol algorithm:

Step1: Source node sent RREQ to all neighbors.

Step2: Source node receives RREP from neighbors.

Step3: Source node select shortest and next shortest path based on the number of hops

Step4: Source node checks its routing table for single hop neighboring nodes only

Step5: If the neighbor node is in its routing table then sent data packet else. The node is malicious (black hole) and sends fake packets to that node.

Step 6: Invoke the route discovery notify all the neighboring nodes about the outsider.

Step 7: Add the status of outsider to the routing table of source node.

Step 8: Again send packet to neighboring node

Step 9: If step 5 repeats then broadcast the malicious node as black hole

Step 10: Update the routing table of source node after every broadcast

Step 11: Repeat step 4 to 10 until packet reaches the destination node correctly.

Black hole attack is a type of active attack [4]. Black hole attack can arise when the malicious node on the path attack the data transfer and purposely drop, delay or change the data transfer passing through it [9]. Black hole node treats itself as a trusted node. Black hole node send false routing information, claim that it has a best route and cause additional good nodes to route data packets through the black hole node. A

black hole node drops all packets that it receives instead of normally forward those packets or message. There are basically two types of black hole attack i.e. internal black hole and External black hole attack [5]. Black hole is a malicious node that wrongly replies for some route requests (RREQ) without having active route to particular destination and drop all the getting packets. If these malicious nodes work jointly as a collection then the damage will be very risky. This type of attack is called cooperative black hole attack.

Internal Black hole attack

In this attack, malicious attack does not try to fit in to active route between source and destination [5]. It is present internally in the network, makes itself active route node in the network [3]. It will be able to attack as the data transmission start between nodes [5].

External Black hole attack

In this, malicious node is externally to the network and stay outside [3]. It creates congestion in the network and disturbs all the working of the network [3]. It can become an internal attack when it take control of internal malicious node and run it to strike other nodes in network [8].

Single Black hole attack

In this attack, single node is behaving as a black hole node and disturbs the entire network functioning [6]. There is only one single node in an area [12]. AODV route discovery method is based on RREQ/RREP messages. Source node broadcast the RREQ message to all its neighbors. Either the target or middle node sends RREP (route reply). The RREP received first by source node is accepted and all further RREPs are not needed. Black hole node takes benefit of this characteristic of AODV and sends RREP (route reply) without checking its routing table. In this way, a route through black hole node is setup and black hole node consumes all the packets and drops all the packets [7].

Route Discovery

Route discovery is the mechanism by which source node discovers route for destination. In route discovery, the source node floods the route request packet throughout the network, and the reply is returned either through the destination node or through any intermediate nodes which contains the route to destination in its route cache. For example, if source Node A wishes to send packet to Destination Node B, it obtains a source route for Node B. This route discovery is initiated only when Node A tries to send packet for Node B and does not find any route in its own route cache. Finding a route for destination will be purely on demand using the route discovery mechanism.

VI. CONCLUSION AND FUTURE SCOPE

This is a review on various protocols standards. In this paper we describe the brief introduction to the many challenges in black hole prevention techniques in MANET. Algorithms that are described in are based on comparison of AODV and DSDV .Wireless networks are characterized by a lack of infrastructure, and by a random and quickly changing network topology; thus the need for a robust dynamic routing protocol that can accommodate such an environment. We have described many of the issues that need to be tackled and that have been left unspecified by the current standards. We identified a number of objectives that any solution should aim at meeting and provided an initial investigation of some of these problems. This is obviously preliminary work and we are actively investigating many of the problems outlined in this paper. We hope that the paper will also entice others in exploring what we feel is a promising and rich research area. After removing this attack from network, it will increase the packet delivery Ratio and decrease the packet dropping ratio and increase the security from black hole attack. In future, we try to more improve the MN-ID method which gives better results.

REFERENCES

[1] Funde N. A., Pardhi P. R., "Detection & *Prevention Techniques to Black & Gray Hole Attacks in MANET: A Survey*", International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 10, October 2013.

[2] Sharma R. , Shrivastava R. , "Modified *AODV Protocol to Prevent Black Hole Attack in Mobile Ad-hoc Network*", IJCSNS International Journal of Computer Science and Network Security, VOL.14 No.3, March 2014.

[3] Kalra J., Kaur R. , "*A Review Paper on Detection and Prevention of Black hole in MANET* " , International Journal of Advanced Research in Computer Science and Software Engineering ,Volume 4, Issue 6, June 2014.

[4] Singh R. , Sharma A., Pandey G., "Detection *and Prevention from Black Hole attack in AODV protocol for MANET*", International Journal of Computer Applications (0975 – 8887), Volume 50 – No.5, July *2012.*

[5] Baadache.A , Belmehdi.A , "Avoiding Black hole and Cooperative Black hole Attacks in Wireless Ad hoc Networks" , (IJCSIS) International Journal of Computer Science and Information Security, *Vol. 7, No. 1, 2010.*

[6] Phyu.T, Khin.E, "Impact Of black hole attack on AODV Protocol", International Journal of Information Technology, Modeling and Computing (IJITMC) Vol. 2, No.2, May 2014

[7] http://ijcem.org/papers12011/12011_17.pdf

[8] Pooja, Kumar V. , " *A Review on Detection of Black hole Attack Techniques in MANET*" , International Journal of Advanced Research in Computer Science and Software Engineering ,Volume 4, Issue 4, April 2014.

[9] Saini.A, Kumar.H, "Effect Of Black Hole Attack On AODV Routing Protocol In MANET", IJCST Vol. 1, Issue 2, December 2010.

[10] Patel.A et. al., "Effect of Black Hole Active Attack on Reactive Routing Protocol AODV in MANET using Network Simulator" International Journal of Electronics and Computer Science Engineering ISSN- 2277-1956.

[11] Saini.A, Kumar.H, "Effect Of Black Hole Attack On AODV Routing Protocol In MANET", IJCST Vol. 1, Issue 2, December 2010.

[12] Phyu.T, Khin.E, "Impact Of black hole attack on AODV Protocol", International Journal of Information Technology, Modeling and Computing (IJITMC) Vol. 2, May 2014