ISSN XXXX XXXX © 2017 IJESC

Research Article Volume 7 Issue No.5

Multiple Black Hole Detection Algorithm for AODV in MANET

Pooja Rani
M.Tech Scholar
Department of Computer Science & Engineering
Bhagat Phool Singh Mahila Vishwavidyalaya, Khanpur Kalan, Haryana, India

Abstract:
When multiple devices (nodes) perform communication wirelessly & share network features with each other then they form an ad hoc wireless network. These communications is performed without establishing any central administrator. The wireless nodes that can dynamically form a network to exchange information without using any existing fixed network infrastructure. When nodes which are performing communication are mobile nodes (i.e., moves from one location to another) then it is called a Mobile Ad hoc Network (MANET). In a MANET, communication between the mobile devices is carried out by some intermediate devices called routers. In the routing of MANET, some intermediate nodes act maliciously & attack the packets that are delivered through them. One such type attack is black hole attack that absorbs all data packets in the network without moving them to forward. Hence data loss will occur as data packets are not moved to the destination node. In this paper, we provide a secure mechanism to overcome such types of attacks. We provide modified algorithm for black hole attack which will help to detection of multiple black hole attacks.

Keywords: MANET, Black hole attack, end to end acknowledge

I. INTRODUCTION

Wireless ad-hoc networks [1] are composed of autonomous nodes that are self- managed without any infrastructure. Therefore, nodes in ad-hoc networks can enter and leave the network dynamically. This network is generally established in an area where a fixed infrastructure is impossible. The nodes communicate with each other by passing the packets of message through each other.

The ad-hoc network uses some routing protocol for proper transfer of packets from source to destination. Some popular protocols are – Dynamic Source Routing (DSR), Ad-hoc On-Demand Distance Vector (AODV) & Destination-Sequenced Distance-Vector (DSDV). The Mobile Ad-hoc Networks are used in numerous applications-in military and rescue areas, to establish a new network after any natural calamity. Besides acting as a host, each node also acts as a router to discover a path and forward packets to the correct node in the network.

As wireless ad-hoc networks lack an infrastructure, they are exposed to a lot of attacks. One of these attacks is the Black Hole attack [2] [3].

In the Black Hole attack, a malicious node absorbs all data packets in itself, similar to a hole which sucks in everything in. In this way, all packets in the network are dropped. A malicious node dropping all the traffic in the network makes use of the vulnerabilities of the route discovery packets of the on-demand protocols, such as AODV.

In route discovery process of AODV protocol, intermediate nodes are responsible to find a fresh path to the destination, sending discovery packets to the neighbor nodes.

Malicious nodes do not use this process and instead, they immediately respond to the source node with false information as though it has fresh enough path to the destination. Therefore, source node sends its data packets via the malicious node to the destination assuming it is a true path.

Black Hole attack may occur due to a malicious node which is deliberately misbehaving, as well as a damaged node interface. In any case, nodes in the network will constantly try to find a route for the destination, which makes the node consume its battery in addition to losing packets. Our mechanism helps to protect the network by detecting and reacting to malicious activities of any node.

In first section, we specified introduction of manet and black hole in second section, we are discussing routing protocol in manet. In third section, we tell about black hole attacks. In fourth section, we are discussing about multiple black hole attacks and proposed solution for detecting multiple black hole attacks.

II. ROUTING IN MANETS

MANETs have special limitation and properties such as limited bandwidth and power, highly dynamic topology, high error rates etc. [2][4].

Moreover, compared to infrastructure based networks, in a MANET, all nodes are mobile and can be connected dynamically in an arbitrary manner. Nodes of MANET behave as router and take part in discovery and maintenance to establish a reliable route of each other.

Therefore, routing protocols for wired networks cannot be directly used in wireless networks and numerous protocols have been developed for MANETs.

These routing protocols are divided into two categories based on management of routing tables. These categories are Table Driven Routing Protocols and On-Demand Routing Protocols, shown in the Table 1 below.

Table.1. MANET Routing Protocols

Table Driven Routing Protocols	**On-Demand Routing Protocols**
Destination-Sequenced Distance Vector Routing Protocol (DSDV)	Ad-Hoc On-Demand Distance Vector Routing (AODV)
Wireless Routing Protocol (WRP)	Cluster based Routing Protocols (CBRP)
Global State Routing (GSR)	Dynamic Source Routing Protocol (DSRP)
Hierarchical State Routing (HSR)	Associativity Based Routing (ABR)
Zone-based Hierarchical Link State Routing Protocol (ZHLS)	Signal Stability Routing (SSR)
Fisheye State Routing (FSR)	Temporally Ordered Routing Algorithm (TORA)

Ad-hoc On-Demand Distance Vector (AODV) [8] Routing Protocol is used for finding a path to the destination in an ad-hoc network. To find the path to the destination all mobile nodes work in cooperation using the routing control messages. Thanks to these control messages, AODV Routing Protocol offers quick adaptation to dynamic network conditions, low processing and memory overhead, low network bandwidth utilization with small size control messages.

The most distinguishing feature of AODV compared to the other routing protocols is that it uses a destination sequence number for each route entry. The destination sequence number is generated by the destination when a connection is requested from it. Using the destination sequence number ensures loop freedom. AODV makes sure the route to the destination does not contain a loop and is the shortest path. Route Requests (RREQs), Route Replay (RREPs), Route Errors (RERRs) are control messages used for establishing a path to the destination, sent using UDP/IP protocols. Header information of these control messages are explained in [9]. When the source node wants to make a connection with the destination node, it broadcasts an RREQ message. This RREQ message is propagated from the source, received by neighbors (intermediate nodes) of the source node. The intermediate nodes broadcast the RREQ message to their neighbors. This process goes on until the packet is received by destination node or an intermediate node that has a fresh enough route entry for the destination. While the RREQ packet travels through the network, every intermediate node increases the hop count by one.

III. BLACK HOLE ATTACK

Black hole attack is network layer attacks which have dropped all the packet by sending fake packet to source node or other node. To carry out a black hole attack, malicious node waits for neighboring nodes to send RREQ messages. When the malicious node receives an RREQ message, without checking its routing table, immediately sends a false RREP message giving a route to destination over itself, assigning a high sequence number to settle in the routing table of the victim node, before other nodes send a true one.

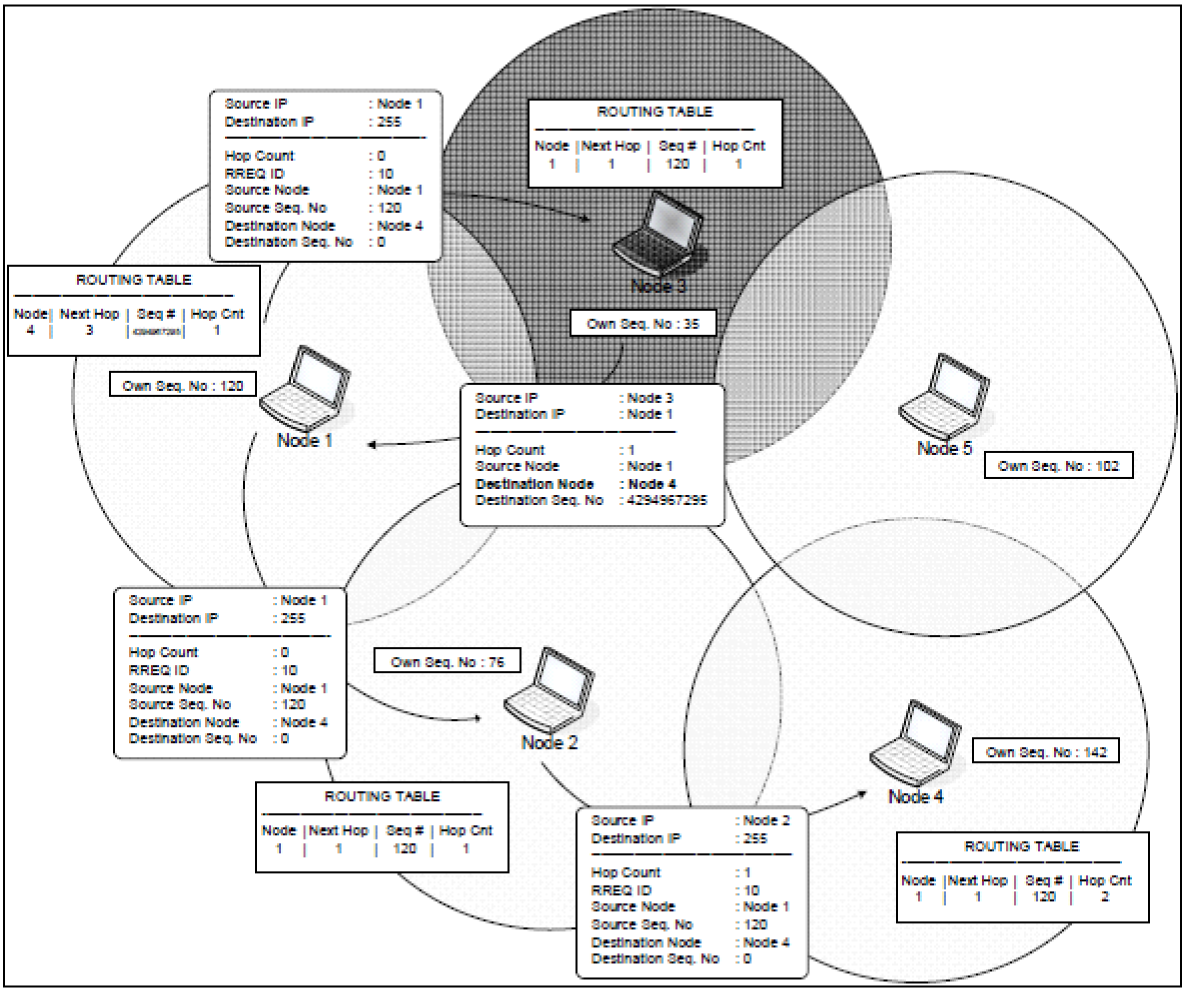
Therefore, requesting nodes assume that route discovery process is completed and ignore other RREP messages and begin to send packets over malicious node. Malicious node attacks all RREQ messages this way and takes over all routes.

Therefore, all packets are sent to a point when they are not forwarding anywhere. This is called a black hole akin to real meaning which swallows all objects and matter. To succeed a black hole attack, malicious node should be positioned at the center of the wireless network. If malicious node masquerades false RREP message as if it comes from another victim node instead of itself, all messages will be forwarded to the victim node.

By doing this, victim node will have to process all incoming messages and is subjected to a sleep deprivation attack [11]. *Behavior of black hole attack in AODV-* In an ad-hoc network that uses the AODV protocol, a Black Hole node absorbs the network traffic and drops all packets.

To explain the Black Hole Attack, we added a malicious node that exhibits Black Hole behavior in the scenario as shown in figure 2 below. In this scenario, we assume that Node 3 is the malicious node. When Node 1 broadcasts the RREQ message for Node 4, Node 3 immediately responds to Node 1 with an RREP message that includes the highest sequence number of Node 4, as if it is coming from Node 4. Node 1 assumes that Node 4 is behind Node 3 with 1 hop and discards the newly received RREP packet come from Node 2. Afterwards Node 1 starts to send out its data packet to the node 3 trusting that these packets will reach Node 4 but Node 3 will drop all data packets.

In a Black Hole Attack, after a while, the sending node understands that there is a link error because the receiving node does not send TCP ACK packets. If it sends out new TCP data packets and discovers a new route for the destination, the malicious node still manages to deceive the sending node. If the sending node sends out UDP data packets the problem is not detected because the UDP data connections do not wait for the ACK packets.



Source IP : Node 1
Destination IP : 255
Hop Count : 0
RREQ ID : 10
Source Node : Node 1
Source Seq. No : 120
Destination Node : Node 4
Destination Seq. No : 0

ROUTING TABLE

Node	Next Hop	Seq #	Hop Cnt
1	1	120	1

ROUTING TABLE

Node	Next Hop	Seq #	Hop Cnt
4	3	[illegible]	1

Source IP : Node 3
Destination IP : Node 1
Hop Count : 1
Source Node : Node 1
Destination Node : Node 4
Destination Seq. No : 4294967295

Source IP : Node 1
Destination IP : 255
Hop Count : 0
RREQ ID : 10
Source Node : Node 1
Source Seq. No : 120
Destination Node : Node 4
Destination Seq. No : 0

ROUTING TABLE

Node	Next Hop	Seq #	Hop Cnt
1	1	120	1

Source IP : Node 2
Destination IP : 255
Hop Count : 1
RREQ ID : 10
Source Node : Node 1
Source Seq. No : 120
Destination Node : Node 4
Destination Seq. No : 0

ROUTING TABLE

Node	Next Hop	Seq #	Hop Cnt
1	1	120	2

V. MULTIPLE BLACK HOLE ATTACK

In multiple black hole attack, there are more than one black hole nodes that drop the data packets. In AODV, There is no direct path from source to destination; the nodes cooperate with each other for sending the data packets. The source node broadcasts RREQ packets to all the neighbor nodes for the establishment of routing path between source and destination. The intermediate nodes which have the shortest path towards destination sends RREP packet to the source. The sequence number is used to decide the freshness of the route. The highest sequence number refers to the fresh route. The black hole node advertises itself as it has the shortest path from source to destination. When black hole node receives RREQ packet, it sends RREP packet to the source with highest destination sequence number (Figure 1).

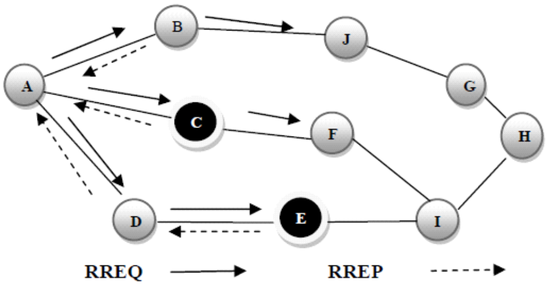


Figure.1. Multiple Black Hole Attack.

The source node then selects the black hole node as intermediate node through which the data packets will be sent. The Black hole nodes can work individually or in group. When black hole nodes work in a group, they are called as cooperative black hole nodes. The black hole node in case of cooperative black hole attack, the black hole nodes work in a group in order to drop the packets. In the first phase, the black hole node exploits the routing protocol such as the AODV or DSR and advertises itself of having the shortest or valid path towards the destination with an intention to drop all the packets. In above figure, the nodes C and E are black hole nodes present in the network. Here, both the black hole nodes work individually in order the drop the data packets. If both black hole nodes work together then it is cooperative black hole attack. When the source chooses that spurious route, the black hole node starts to intercept the data packets in its second phase. In this paper, the detection mechanism is proposed for tackling the multiple black hole nodes problem by modifying the AODV protocol.

VI. PROPOSED ALGORITHM

Pseudo code of proposed method

```
// Data receiving routine
If (Data received on network layer && data->source == index)
{
if (detection mode == false)
Sendrequest(data->dest)
Else
Sendrequest (index)
}
// recv reply routine
Recvreply ()
{
If(blacklist_nodeid ==reply->source)
{
Drop_reply();
}
If(detectionmode)
{
If(reply->dest_seqno> seqno) // Comparison of sequence number
Blacklist (replysource)
Sendnotification (blacklisted_nodeid);
Detectionmode=false;
}
Else
//existing AODV code
}
//Recv notification routine
Recv_notification()
{
Delete route(notification->source)
Blacklist (notification->blacklisted_node)
}
```

VII. CONCLUSION

Mobile ad-hoc networks are composed of autonomous nodes that are self- managed without any infrastructure. Therefore, nodes in ad-hoc networks can enter and leave the network dynamically. This network is generally established in an area where a fixed infrastructure is impossible. The nodes communicate with each other by passing the packets of message through each other. The ad-hoc network uses some routing protocol for proper transfer of packets from source to destination. In the routing of MANET, some intermediate nodes act maliciously & attack the packets that are delivered through them. One such type attack is black hole attack that absorbs all data packets in the network without moving them to forward. Hence data loss will occur as data packets are not moved to the destination node. In this paper, we provide a secure mechanism to overcome such types of attacks. Simulation will be carried out by using network simulator tool to address the problem of detection & prevention of multiple black hole attack in mobile ad-hoc network.

VIII. REFERENCES

[1]. Aarti and Dr. S.S Tyagi, “Study of MANET: Characteristics, Challenges, Application and Security Attacks”, IJARCSSE International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 3, May 2013.

[2]. Umang Singh, “Secure Routing Protocols in mobile Ad hoc networks-A survey and Taxanomy”, International Journal of Reviews in Computing, 30thSeptember 2011, Vol. 7

[3]. Sanjay Ramaswamy, Huirong Fu, Manohar Sreekantaradhya,John Dixon, and Kendall Nygard, ”Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks”, In Proceedings of 2003 International Conference on Wireless Networks (ICWN’03), Las Vegas, Nevada, USA, pp. 570-575.

[4]. Oscar F. Gonzalez, Michael Howarth, and George Pavlou, “Detection of Packet Forwarding Misbehavior in Mobile Ad-Hoc Networks”, Center for Communications Systems Research, University of Surrey,Guildford, UK. Integrated Network Management, 2007. IM '07. 10th IFIP/IEEE International Symposium on May 21, 2007.

[5]. SuklaBanerjee, “Detection/Removal of Cooperative Black and Gray Hole Attack in Mobile Ad-Hoc Networks”, Proceedings of the World Congress on Engineering and Computer Science 2008 WCECS 2008, October 22 - 24, 2008, San Francisco, USA.

[6]. Muhammad Zeshan, Shoab A. Khan, Ahmad Raza Cheema and Attique Ahmed, "Adding Security against Packet Dropping Attack in Mobile Ad Hoc Networks", in 2008.International Seminar on Future Information Technology and Management Engineering, November 2008, pp. 568-572.

[7]. S. Usha, S. Radha, "Co-operative Approach to Detect Misbehaving Nodes in MANET Using Multi-hop Acknowledgement Scheme", in 2009 International Conference on Advances in Computing, Control, and Telecommunication Technologies, December 2009, pp.576-578.

[8]. Marjan Kuchaki Rafsanjani, Zahra Zahed Anvari, Shahla Ghasemi, “Methods of Preventing and Detecting Black/Gray Hole Attacks on AODV-based MANET”, IJCA Special Issue on “Network Security and Cryptography” NSC, 2011