International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 15
May 2018

Black Hole Detection Approaches for AODV in MANET

Meenu & Ashu Bansal
[1]Department of Computer Science Hindu College of Engineering (HCE),
Deenbandhu Chhotu Ram University of Science & Technology (DCRUST), Sonepat
Meenu.vashisth10@gmail.com
[2]Department of Computer Science Hindu College of Engineering (HCE),
Deenbandhu Chhotu Ram University of Science & Technology (DCRUST), Sonepat
Ashubansal.pec123@gmail.com

Abstract*—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.*

***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.

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	On-Demand Routing

International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 15
May 2018

Protocols	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.

If an RREQ message with the same RREQ ID is received, the node silently discards the newly received RREQs, controlling the ID field of the RREQ message. When the destination node or intermediate node that has fresh enough route to the destination receive the RREQ message they create an RREP message and update their routing tables with accumulated hop count and the sequence number of the destination node. Afterwards the RREP message is unicasted to the source node. While the RREQ and the RREP messages are forwarded by intermediate nodes, intermediate nodes update their routing tables and save this route entry for 3 seconds, which is the ACTIVE_ROUTE_TIMEOUT constant value of AODV protocol.

III. SECURITY ATTACKS IN MANET

Security attack is any action that compromises the security of information in an unauthorized way. The attack may alter, release, or deny data. The attacks on the MANETs can be broadly classified into two categories: passive and active attacks. Both passive and active attacks can be made on any layer of the network protocol stack [2][7].

1. *Passive Attacks*: A passive attack attempts to retrieve valuable information by listening to traffic channel without proper authorization, but does not affect system resources and the normal functioning of the network. Passive attacks are very hard to detect because they do not involve any alteration of the data.

2. *Active Attacks*: An active attack attempts to change or destroy the system resources. It gains an authentication and tries to affect or disrupt the normal functioning of the network services by injecting or modifying arbitrary packets of the data being exchanged in the network. An active attack involves information interruption, modification, or fabrication.

A. Gray Hole Attack (Routing Misbehavior)

Gray hole attacks is an active attack type, which lead to dropping of messages. Attacking node first agrees to forward packets and then fails to do so. Initially the node behaves correctly and replays true RREP messages to nodes that initiate RREQ message. This way, it takes over the sending packets. Afterwards, the node just drops the packets to launch a (DoS) denial of service attack. If neighboring nodes that try to send packets over attacking nodes lose the connection to destination then they may want to discover a route again, broadcasting RREQ messages. Attacking node establishes a route, sending RREP messages. This

process goes on until malicious node succeeds its aim (e.g. network resource consumption, battery consumption). This attack is known as routing misbehavior. [5]

Dropping packets is also one of the behaviors of failed or overloading nodes [8]. One should not evaluate every dropping packet action as a selective existence, gray or black hole attack. Actually most routing protocols have no mechanism to detect whether data packets have been forwarded, DSR being the only exception. [10]

B. Black Hole Attack

The difference of Black Hole Attacks [10] compared to Gray Hole Attacks is that malicious nodes never send true control messages initially. 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].

Gray hole attacks [9] against one or two nodes in the network to isolate them, where as black hole attack affects the whole network. Moreover, the malicious node that attempts grayhole attacks cannot be perceived easily since it does not send false messages. Behavior of failed nodes may seem like selfish nodes attacks or gray hole attacks due to dropping of messages. But, since failed nodes cannot fabricate a new control message, they cannot form a black hole attack although they will drop the message later.

IV. Detecting 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.

Types of Black hole attack in AODV

Internal black hole attack: According to its name, the black hole node fits itself between the routes of source and destination. Due to its presence internally, it makes itself an active data route element. Now it is capable of conducting the packet drop attack when the data transmission is started. It is called an internal black hole attack because the malicious node belongs itself to the data route. It is more vulnerable to defend against it due to it is difficult to detect the internal misbehaving node.

External black hole attack: The external black hole node stay outside the network but deny access to network traffic or disrupts the entire network or creates congestion in the network. It can become the internal attack when it takes the control of the any internal malicious node and attacks to other nodes in MANET. The external can explained as:

Detection of black hole

In this work we use the AODV Encryption decryption to detect the Black hole attack. AODV Encryption decryption is modification of AODV protocol to reduce the effect of Black hole attack by adding Encrypt/Decrypt function in AODV protocol.

Encryption function:

```
void Security_packetAgent::encryption(char out[])
{
int i = 0, key = 3;
for (i=0;  i<strlen(out);  i++)
{
out[i] = (out[i] + key) % 128;
}
}
```

Decryption function:

```
void Security_packetAgent::decryption(char out[])
{
int i = 0, key = 3;
for (i=0;  i<strlen(out);  i++)
{
out[i] = (out[i] - key) % 128;
}

}
```

V. 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.

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] Sukla Banerjee , "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

[9] Onkar V.Chandure, V.T.Gaikwad, "Detection & Prevention of Gray Hole Attack in Mobile Ad-Hoc Network using AODV Routing Protocol",

International Journal of Computer Applications (0975 – 8887) Volume 41– No.5, March 2012.

[10] S.V. Vasantha1, Dr. A. Damodaram, "A Defense Model for Black hole and Gray hole attacks in MANET", International Journal of Computer Science and Mobile Computing, IJCSMC, Vol. 3, Issue. 11, November 2014, pg.570 – 576

[11] Monika, Swati Gupta, "Detection and Prevention of Black Hole & Gray hole attack in MANET using Digital signature Techniques", International Journal Of Engineering And Computer Science ISSN:2319-7242 Volume 4 Issue 7 July 2015, Page No. 13268-13272

[12] Vahid Heydari and Seong-Moo Yoo "E2EACK: An end-to-end acknowledgment-based scheme against collusion black hole and slander attacks in MANETs" in Wireless Networks • October 2015.

[13] Dharman.V, Mr. Venkatachalam.G, Ashok Kumar.P, "Detection of Gray Hole Attack in AODV for MANET's by Using Secure Message Digest", International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056 Volume: 03 Issue: 03 | Mar-2016.