International Journal of Current Engineering and Technology
E-ISSN 2277 – 4106, P-ISSN 2347 – 5161

Available at http://inpressco.com/category/ijcet

Research Article

Detection and Isolation of Black Hole Node in MANET

Alfy Augustine†* and Manju James†

†Department of ECE, St. Joseph's College of Engineering and Technology, Palai, Kerala, India

Accepted 16 Oct 2015, Available online 20 Oct 2015, **Vol.5, No.5 (Oct 2015)**

Abstract

Advancement in wireless technologies and improved use of wireless devices demands more infrastructure-less networks like MANET. Security of such a scenario is a challenging task over last few years. Because of its distinctive characteristics such as open medium and dynamic network topology, MANET can be accessible to malicious users. Black hole attack is one of serious threat in mobile ad hoc network, in which malicious node absorbs the packets instead of forwarding them to destination. In the proposed work Black hole attack in the network is detected and eliminated in two phases. Black hole attack is detected using a watchdog mechanism, which is the basis of different Intrusion Detection System (IDS) along with an acknowledgement scheme. After identifying the attack, the proposed system removes black hole node from the path and provide a new route to destination.

Keywords: *MANET, Intrusion Detection System, watchdog, Acknowledgement Scheme*

1. Introduction

Wireless network is a growing new technology that will allow users to access services and information electronically, irrespective of their geographical position. Recent advancement such as blue-tooth introduced a new wireless system known as MANET, Mobile Ad hoc Network to establish communication between mobile nodes via radio waves. Mobile Ad hoc Network is a group of wireless mobile nodes in which nodes collaborate by forwarding packets for each other to allow them to communicating outside range of direct wireless transmission (Sukhpreet Kaur, *et al*, 2013).

MANET doesn't need any fixed infrastructure. The network should detect any new node automatically, that enters the network. Conversely, if a node moves out of the network, remaining nodes reconfigure themselves to adjust to the new scenario.

MANET are vulnerable to different DoS attack and prevention of such attack is a challenging issue. Most of the attacks in the MANET are launched by exploiting the Routing Protocol used in the network. In case of critical data or high confidential information, data may be encrypted using cryptographic keys and is send through the network. But prevention methods such as authentication and encryption, which is used as the first line of defense, are commonly used for reducing possibilities of attacks. They are not enough to make MANET secure because of its unique characteristics (Alfy Augustine, *et al*, 2015).

So mitigating of all the attacks from the network requires the routing protocol to be aware of such attacks and defend against such possible attacks in the network.

In this paper, the Black hole attack in MANET is discussed and analyzed. The objective of the work is to find an effective mechanism to detect and eliminate black hole attack from the network.

This paper is organized as follows: Section 2 provides a brief detail on AODV Routing Protocol. Section 3 describes about black hole in MANET. Detection and isolation method is given in section 4. Conclusion on detection mechanism is described under section 5.

2. Ad hoc On Demand Distance Vector (AODV)

Ad hoc On Demand Distance Vector (AODV) is a reactive routing protocol which establish route between mobile nodes only when it is needed. AODV generates three types of messages: Route Request (RREQ), Route Reply (RREP) and Route Error (RERR) (Luke Klein-Berndt). In order to initiate route discovery process RREQ messages are used.

Fig.1 shows the working of AODV routing protocol. When a source node needs a route to destination, it generates a RREQ packet across the network. Several information like source address, destination address, hop count and destination sequence number are included in RREQ message.

*Corresponding author **Alfy Augustine** is a PG Scholar and **Manju James** is working as Assistant Professor

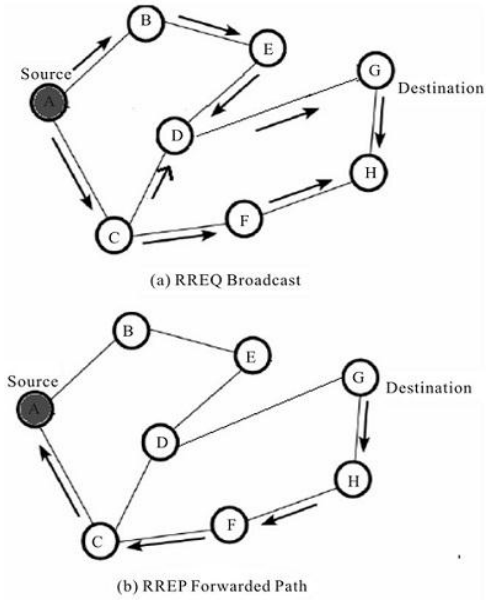

Fig.1 AODV Routing Protocol

Routes are finalized by using RREP message. When a source node receive RREQ message it have two choices, either it can send a RREP message back to source node if they know route to destination or they will rebroadcast the RREQ message to their neighbors. The RREQ keeps getting rebroadcast until the hop count is up. AODV also generates a RERR message to adjust to the routes whenever there occurs an error in route.

AODV is a widely used reactive routing protocol as it discovers optimum routes with low delay. The only problem with AODV is that, they are highly vulnerable to different types of attacks like black hole attack.

3. Black Hole Attack

Black Hole attack is a kind of Denial of Service attack in mobile ad hoc network, in which all data packets are absorbed by the malicious node (Bo Sun Yong Guan, *et al*, 2003). Black hole attack is introduced in the route discovery process of AODV routing protocol.

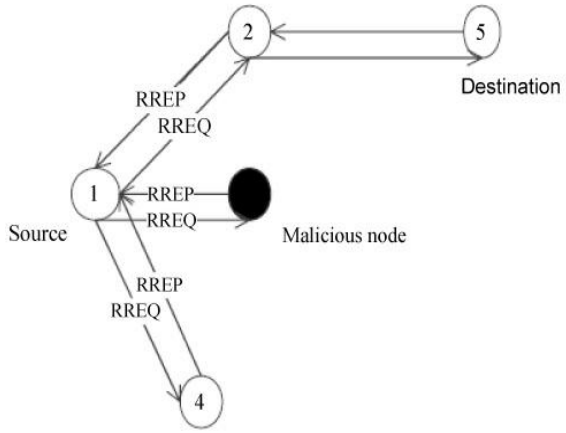

Fig.2 Black Hole Attack

Figure 2 shows the black hole attack. Here 1 is source node and 5 is destination node. Node 1 wants to send a packet to node 5. So node 1 starts with route discovery process by broadcasting a Route Request message across the network. Hearing this malicious node claims it has the shortest route to the destination. Since the Route Reply message from the malicious node is more likely to reach the source node first, source node ignore all other reply messages and begin to send data packets to the malicious node, thinking that the route discovery process is complete. As a result all the data packets are absorbed by malicious node. Once the forged route has been established the malicious node is able to become a member of the active route and intercept the communication packets.

Black hole attacks are of two types: Single Black hole attack and Cooperative Black hole attack. In single black hole attack, one node advertises itself having the shortest route to the destination and intercepts the packet. In cooperative black hole attack, malicious nodes act in groups.

4. Detection and Elimination of Black Hole

In order to detect black hole attack, a mechanism based on watchdog has been designed. Watchdog (S. Marti,, *et al,* 2000) detect misbehavior nodes by monitoring the transmission of next hop neighbor. In watchdog, the copy of the packets that are forwarded by a node are kept in a buffer and it eavesdrop on the transmission of next link to confirm that it forwards packet properly. The overheard packet is then compared with the packet that is kept in buffer. The packet in the buffer is removed if there is a match. Otherwise, the watchdog increments the failure count of the node which is responsible for forwarding packets. The node is detected as misbehaving node when the failure count exceeds some threshold value and a notification message is sent to source node.

The watchdog mechanism is based on passive overhearing (K. Liu, *et al,* 2007). i.e., it can only identify whether or not next hop neighbor send packets. It cannot tell the reception status of receiver. In order to solve this issue, a scheme based on acknowledgement of packets (T. Sheltami, *et al*, 2009) has been designed. In this scheme, when the source node forwards a packet, it waits for an acknowledgement packet from destination node. When the destination node receives a packet it sends back an acknowledgement back to source node through each node along the reverse route. The packet transmission is successful if source node receives an acknowledgement packet. Otherwise an alarm message is generated (Alfy Augustine, *et al*, 2015).

When a Black hole attack is detected, the information about black hole nodes are propagated across the network and they are not considered by any node in further route discovery processes. What we are basically doing here is, if the path to destination contains a black hole node, then delete that route to the destination, because it contains the route via black

hole node. Now, there is no route to destination, so On demand AODV will find a new path to destination via initiating a Route Discovery process. During that time, black hole node is prevented from getting added in the new route. It is done by dropping the RREP from black hole node and restricts them by not adding to routing table. So the new path to destination is free from black hole node.

4.1 Implementation Methodology

NS2 (Network Simulator-2) is used for simulation. The Structure of MANET in NS-2 is shown in Table 1.

Table 1 MANET Configuration in NS2

Protocol	AODV
Mac layer	IEEE 802.11
Transmission range	250 m
Node placement	Random
Area	900m X 900m
Size of data packets	512 bytes
No. of nodes	20
Traffic type	CBR
Simulation time	100 sc

4.2 Simulation Results

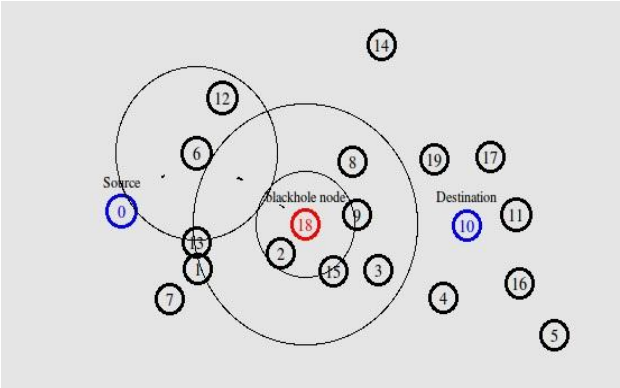

Fig.3 Network Scenario with Black hole attack

Fig.3 shows the network scenario when there is a black hole attack. Here node 18 is set as black hole node. Detection of black hole node is done by adding watchdog to AODV routing protocol. When a black hole node is detected, it generates an alarm message to source node. Detection of attacker node is shown in Fig. 4.

```
Node: _13 _ recvd data packet
Node: _18 _ recvd data packet The node 18 (18) starts a blackhole

Node: _0 _ recvd data packet
Node: _13 _ recvd data packet
Node: _18 _ recvd data packet
Node: _0 _ recvd data packet
Node: _13 _ recvd data packet
Node: _18 _ recvd data packet superuser@superuser-VPCEH25EN:~$
```

Fig.4 Watchdog detects Black hole attack

From the figure it is clear that, when a black hole initiates in the network it absorbs the entire packet and node 10, the destination node, doesn't receive any packet. Fig.5 shows the forwarding of acknowledgement packets back to source node when the destination receives the packet.

```
( 0) - 10 sending Route Request, dst: 137327324
channel.cc:sendUp - Calc highestAntennaZ_ and distCST_
highestAntennaZ_ = 1.5,  distCST_ = 550.0
SORTING LISTS ...DONE!
sending Reply from 10 at 0.41
sending ACK from 10 at 0.42
3 - recvACK: received an ACK at 0.42
sending ACK from 10 at 0.42
18 - recvACK: received an ACK at 0.42
sending ACK from 10 at 0.43
13 - recvACK: received an ACK at 0.43
sending ACK from 10 at 0.43
0 - recvACK: received an ACK at 0.43
```

Fig.5 Acknowledgement of packets

When node 10 receives data packet, it send an acknowledgement packet back to node 0 through the nodes 13, 18 and 3. If there is black hole attack, node 10 doesn't receive any packet. So in this case, acknowledgement packets are not generated. Table 2 shows the routing table with black hole attack.

Table 2 Routing Table with black hole

Node Id	Destination	Next hop
0	10	13
13	10	18
18	10	3
3	10	10

When a Black hole attack is detected, the information about black hole nodes are propagated across the network and they are not considered by any node in further route discovery processes. If the path to destination contains a black hole node, then delete that route to the destination from routing table. In this case AODV will find a new route to destination. Fig. 6 shows the proposed system finds a new path to destination which is free from black hole.

```
Node: _0 _ recvd data packet
Node: _13 _ recvd data packet
Node: _18 _ recvd data packet The node 18 (18) starts a blackhole at 6.016316 secs!

Node: _13 _ recvd data packet
Node: _0 _ recvd data packet
Node: _1 _ recvd data packet
Node: _9 _ recvd data packet
Node: _10 _ recvd data packet
Node: _9 _ recvd data packet
Node: _0 _ recvd data packet
Node: _1 _ recvd data packet
Node: _9 _ recvd data packet
Node: _10 _ recvd data packet
```

Fig.6 Black hole Elimination

In this case the destination node, node 10, receives packet through nodes 1 and 9. On receiving data packet node 10 generates an acknowledgement packet and sends to source node, node 0, through nodes 9 and 1.

```
 sending ACK from 10 at 21.12
9 - recvACK: received an ACK at 21.12

 sending ACK from 10 at 21.12
1 - recvACK: received an ACK at 21.12

 sending ACK from 10 at 21.13
0 - recvACK: received an ACK at 21.13
```

Fig.7 Acknowledgement of packets

Fig. 7 shows the forwarding of acknowledgement packets through new path. Table 3 shows the routing table of proposed method.

Table 3 Routing Table with black hole elimination

Node Id	Destination	Next hop
0	10	1
1	10	9
9	10	10

4.3 Performance Analysis

Evaluation of the proposed system is done using some selected metrics and the effects of normal AODV under black hole attack are compared against that of the proposed method. Performance metrics used to evaluate the performance of proposed system are:

1) Packet Delivery Ratio

It is the ratio of the packets that are successfully delivered to the destination.

Packet Delivery Ratio
= Number of packet sreceived
/Number of packets send

2) End-to-End Delay

It is the average time taken by the packets to pass through the network.

$$\text{End} - \text{to} - \text{End delay [packet id]} = \text{received time[packet id]} - \text{sent time[packet id]}$$

3) Throughput

It is the amount of data transferred over the period of expressed in bits per second.

Throught (bits per second)= (No. of delivered packets*Packet size*8)/(Simulation time)

Table 4 Simulation Results

Parameter	Packet Delivery Ratio	End-to-End Delay(ms)	Throughput (Kbps)
Without Black hole	1.29619	0.7129	13.65
Proposed work	6.06729	0.14436	61.94

Table 4 shows the simulation results. In the presence of black hole attack, normal AODV cannot detect these attacks and uses a malicious path for packet forwarding.

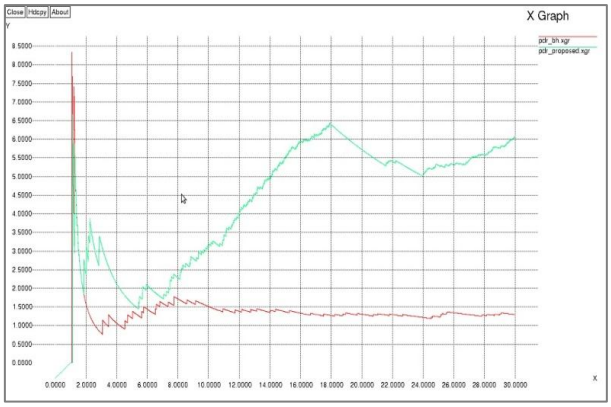

Fig.8 Packet Delivery Ratio

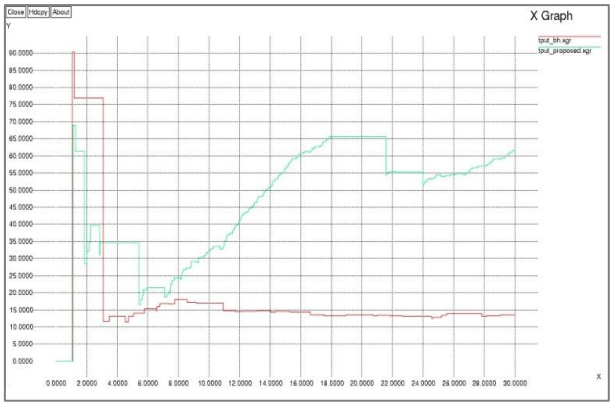

Fig.9 Throughput

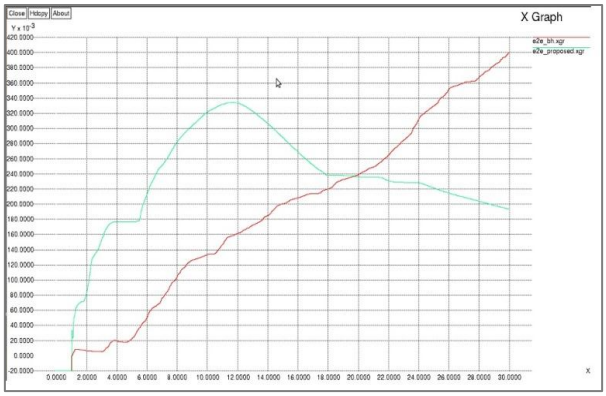

Fig.10 End-to-End Delay

These paths having black hole node will attract all the packets in the network and deliberately drop them, which results in low packet delivery Ratio and throughput. Figures 8, 9 and 10 respectively show the X graph of packet delivery ratio, throughput and end to end delay. From the figure, it is clear that the proposed system have high packet delivery ratio and throughput as this system detects the black hole attack along the route and finds a safe route to destination and also have a low end to end delay.

Conclusions

MANET which is a promising area of research, are vulnerable to many security threats. One of them is black hole attack. The proposed system detects black hole attack by using watchdog and generates an alarm message across the network, if it detects an attack. The reception of the packet by the receiver is verified by sending an acknowledgement packet back to source node. The information about blacklisted nodes are propagated across the network and they are not considered by any node in further route discovery processes. Performance is evaluated based on throughput, Packet Delivery Ratio and End-to-End Delay. The performance analysis is done by comparing the normal AODV with the proposed system, in the presence of a black hole attack. The throughput and packet delivery ratio increases in proposed method compared to normal AODV with black hole and end to end delay decreases drastically on using the proposed system. This method can effectively remove black hole attackers from the network and hence provide security of data transmission in the network. This method can be extended to detect other attacks like wormhole attack; DOS etc. shall be carried out for advance research

References

Sukhpreet Kaur, Chandan Sharma, (2013), An Overview of Mobile Adhoc Network*, Ericsson, IOSR-JCE*, Vol. 11 No. 4.

Alfy Augustine, Manju James, (2015), Black Hole Detection Using Watchdog, *International Journal of Current Engineering and Technology,* Vol. 5, No. 4.

Ramanpreet Kaur, Anantdeep Kaur, (2014), Blackhole Detection In MANETS Using Artificial Neural Networks, *International Journal for Technological Research in Engineering*, Vol. 1,Issue. 9.

Tiranuch Anantvalee, Jie Wu, (2006), A Survey on Intrusion Detection in Mobile Ad Hoc Networks, Wireless/Mobile Network Security, *Springer*, pp. 170 - 196.

Luke Klein-Berndt, A Quick Guide to AODV Routing , National Institute of Standards and Technology.

Bo Sun Yong Guan, Jian Chen Udo W. Pooch, (2003), Detecting Black-hole Attack in Mobile Ad Hoc Networks, *EPMCC*.

S. Marti, T. J. Giuli, K. Lai, and M. Baker., (2000), Mitigating routing misbehaviour in mobile ad hoc networks in Proc. 6th *Annu. Int. Conf. Mobile Comput. Netw*., Boston, MA, pp. 255265.

K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan, (2007), An acknowledgment-based approach for the detection of routing misbehaviour in MANETs, *IEEE Trans. Mobile Comput*., vol. 6, no. 5, pp. 536550.

T. Sheltami, A. Al-Roubaiey, E. Shakshuki, and A. Mahmoud, (2009), Video transmission enhancement in presence of misbehaving nodes in MANETs, *Int. J. Multimedia Syst.,* vol. 15, no. 5, pp. 273282.

Moradi Zahra, Teshnehlab M., Rahmani A. M., (2011), Implementation of Neural Networks for Intrusion Detection in MANET , *IEEE Trans*.

Nidhi Lal, (2010), An Effective Approach for Mobile ad hoc Network via I-Watchdog Protocol, *International Journal of Artificial Intelligence and Interactive Multimedia*, Vol. 3.

Kanika Lakhani ,Himani bathla, Rajesh Yadav, (2010), A Simulation Model to Secure the Routing Protocol AODV against Black-Hole Attack in MANET, *IJCSNS, International Journal of Computer Science and Network Security*, Vol.10, No.5.

Surana K.A., Rathi S.B. Thosar T.P. and SnehalMehatre, (2012), Securing Black Hole Attack in Routing Protocol AODV in MANET with Watchdog Mechanisms, *World Research Journal of Computer Architecture* , Vol. 1 Issue 1, pp. 19-23.

Dais John, Rosna P Haroon, (2014), Selfish Node Isolation and Incentivation using Progressive Thresholds, *ACEEE Int. J. on Network Security*,Vol.5.