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

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

Research Article

Black Hole Detection using Watchdog

Alfy Augustine†* and Manju James†

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

Accepted 01 Aug 2015, Available online 05 Aug 2015, **Vol.5, No.4 (Aug 2015)**

Abstract

Security related issues are of serious concern in MANET. Shared wireless medium and lack of central administration makes MANET more vulnerable to security threats. An intruder passes an intermediate node into the MANET and introduces several kinds of attacks on the data transfer occurring between nodes. If the MANET can detect those attackers as soon as they enter the network, then the consequences caused by those compromised nodes can be minimized. In this paper we consider Black hole attack in mobile ad hoc network, where all data packets are absorbed by the malicious nodes. In order to detect Black hole attack, a watchdog mechanism, which is the basis of different Intrusion Detection System (IDS) has been designed along with an acknowledgement scheme.

Keywords: *MANET, Intrusion Detection System, watchdog.*

1. Introduction

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. They are capable of operating without the aid of any fixed infrastructure. The mobile nodes that are in radio range of each other can communicate directly whereas others need the help of intermediate nodes which serve as routers. These networks are fully distributed and can be built at any place. Each node can send traffic and hence the node can act as both a router and a host. Due to Dynamic topology, autonomous terminal, multi hop routing, and self organization MANET find applications in several areas particularly in military tactical, disaster area network and instant conferences (Magnus Frodigh, *et al*, 2000).

Availability, confidentiality, integrity, authentication and non-repudiation are the five major security goals required to maintain a reliable, better and secure ad hoc network environment (Ramanpreet Kaur, *et al*, 2014). Due to their inbuilt characteristics of dynamic topology, lack of central administration and shared wireless medium make MANET susceptible to various security threats. Attacks in MANET are mainly classified into two types: passive attack and active attack. Passive attack does not alter the data transmitted within the network whereas active attack prevents the message flow between the networks. Eavesdropping, traffic analysis and monitoring are the different types of passive attacks. Active attacks include wormhole attack, black hole attack, greyhole, Dos attack, Sybil and rushing attack.

Prevention methods such as authentication and encryption, which is used as the first line of defense, are commonly used for reducing possibilities of attacks. But they are not enough to make MANET secure because of its unique characteristics. Therefore detection should also be added. i.e., the damages caused by compromised nodes in the network can be eliminated, if the MANET can detect those nodes as soon as they enter the network. Here is where the Intrusion Detection System comes in. Intrusion detection can be defined as a process of monitoring activities in a system, which can be a computer or network system. The mechanism by which this is achieved is called an intrusion detection system (IDS) (Tiranuch Anantvalee, *et al*, 2006).

In this paper, the Black hole attack in MANET is discussed and analyzed. Our aim is to design a mechanism based on watchdog to detect black hole attack in the network. An acknowledgement scheme is also designed along with watchdog.

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 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

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

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.

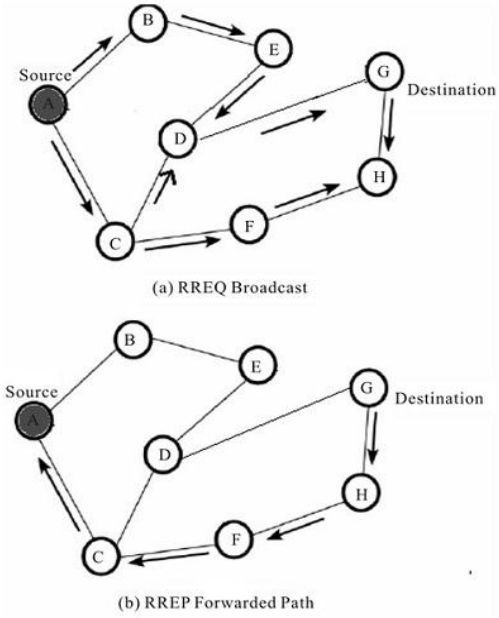

Fig.1 AODV Routing Protocol

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. 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.

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.

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.

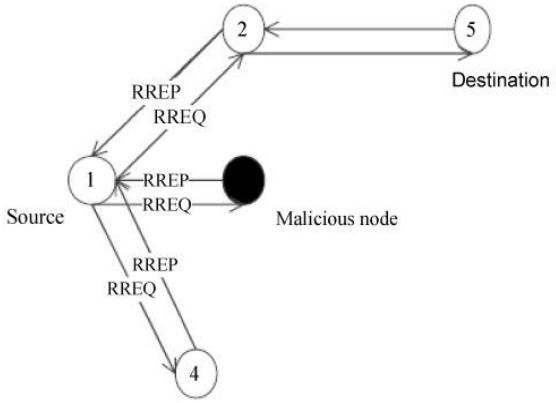

Fig.2 Black Hole Attack

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. Black Hole Attack Detection Method

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.

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

We have performed the black hole attack on AODV routing protocol and compared it with the network without black hole. Then watchdog is implemented by modifying AODV routing protocol. The network is constructed with 20 nodes. The traffic type used here is CBR

4.2 Simulation Results and Analysis

To evaluate the black hole attack we consider the following three metrics:

A. Packet Delivery Ratio

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

$$\text{Packet Delivery Ratio} = \text{Number of packet}\frac{\text{sreceived}}{\text{Number}}\text{of packets send}$$

B. End-to-End Delay

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

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

C. Throughput

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

$$\text{throught(bits per second)} = \frac{\text{No. of delivered packets} * \text{Packet size} * 8}{\text{Simulation time}}$$

Fig.3 shows the network scenario created without black hole.

Using the trace file, performance metrics are calculated and simulation results are shown in table 2.

Table 2 Simulation Results

Parameter	Packet Delivery Ratio	End-to-End Delay	Throughput
Without Black hole	9.0183	0.1305	624.77
With Black hole	5.2752	0.0676	305.79

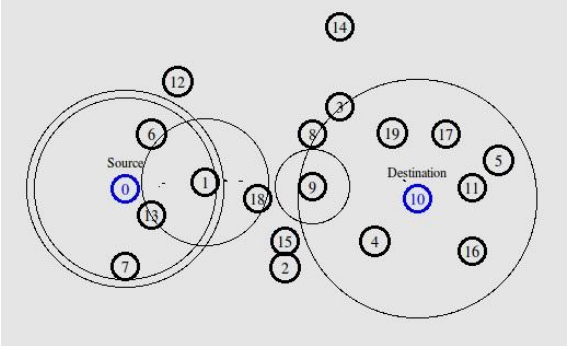

Fig.3 Network Scenario without Black hole attack

From this it is clear that when black hole initiates in the network, there is a decrease in throughput, packet delivery ratio and end-to-end delay. Fig.4 shows the network scenario when there is a black hole attack.

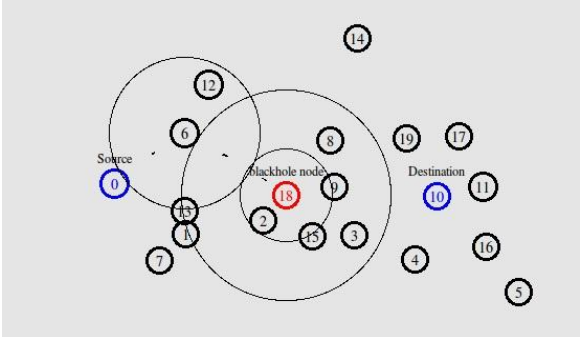

Fig.4 Network Scenario with Black hole attack

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.5.

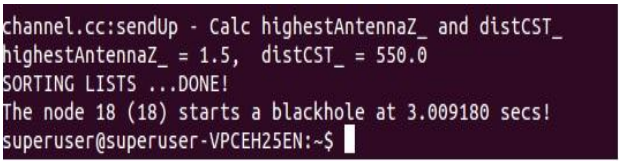

Fig.5 Watchdog detects Black hole attack

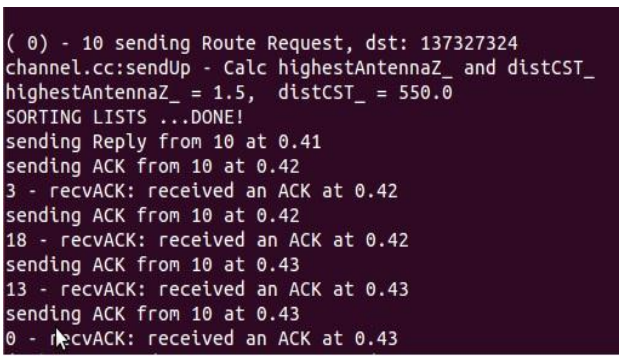

Fig.6 Acknowledgement of packets

Fig.6 shows the forwarding of acknowledgement packets back to source node when the destination receives the packet. i.e., here source node is set as node 0 and destination node is 10. When node 10 receives data packet, it send an acknowledgement packet back to node 0 through the nodes 3, 8 and 13.

If node 18 acts as black hole node, it absorbs the entire packet and node 10, the destination node, doesn't receive any packet. So in this case, acknowledgement packets are not generated.

Conclusions

MANET which is a promising area of research, are vulnerable to many security threats. One of them is black hole attack. In this paper the black hole attack is analyzed and a mechanism is designed based on watchdog to detect black hole node. It is seen that when a black hole initiates in the network, there is a decrease in throughput, packet delivery ratio and end-to end delay. When an attacker enters the network, it is detected by using watchdog and generates an alarm message across the network. The reception of the packet by the receiver is verified by sending an acknowledgement packet back to source node. The model can effectively detect black hole node in the network

References

Magnus Frodigh, Per Johansson and Peter Larsson,(2000), Wireless ad hoc networking the art of networking without a network*, Ericsson Review,* 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.