ISSN: 2277-9655
Impact Factor: 1.852

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

A Survey on Blackhole Attack Detection Methods in Manet

T.Ramesh[*1], T.Jothimani[2]

[*1]Assistant Professor, Department of Information Technology, Bharathiar University, India, Coimbatore-641046, India

[2]Research Scholar, Department of Information Technology, Bharathiar University, India, Coimbatore-641046, India

trcsebu@gmail.com

Abstract

The mobile ad hoc network is the wireless network. MANET is gaining technology because users want to use wireless devices. It is a group of mobile devices connected by wireless link with no access point. Every mobile device in a network is independent. The mobile devices are easy to move randomly and organize themselves arbitrarily. The each mobile node is responsible for routing the message from one node to the other like a router, cause network more vulnerable to the different attacks. Security has become a primary challenge issues in ad hoc network. Black hole attack is one of the security issue in which the traffic is redirected to such a node that actually does not exist in the network. The black hole attack in network traffic connecting the victim node and attack node then network is most important issue that needs efficient solutions. This paper discusses about the Black hole attack detection technique.

Keywords: Mobile Ad hoc network, Black hole attack, Cooperative Black hole attack.

Introduction

A mobile ad hoc network is a collection of mobile nodes that using wireless network to correspond with each other lacking static infrastructure. Mobile devices are act as a host and router. Network nodes are mobile and know how to communicate dynamically in an arbitrary approach. The network is characterized by the lack of central administration devices such as base stations and access points. The network Security in Mobile Ad-Hoc Network (MANET) is the most important concern for the basic functionality of network. Accessibility of network services, privacy and integrity of the data can be achieved by assuring that security issues have been met. This paper focus on black hole attack and different methods are used to detect black hole attack.

Characteristics of Manet

The mobile ad hoc network is highly flexible and robust. It has several characteristics [1].

A. Dynamic Topologies

Nodes are free to move about randomly; therefore the network topology which is typically multi-hop, may change randomly and rapidly at unpredictable times, and may consist of both bidirectional and unidirectional links.

B.Bandwidth-Constrained, Variable Capacity Links

Wireless links will continue to have significantly lower capacity than their hardwired counter parts. In addition the realized throughput of wireless communications after accounting for the effects of multiple access and fading, noise, interference condition and so on. It is often much less than radio's maximum transmission rate.

C. Energy-Constrained Operation

The nodes in MANET can rely on batteries or other exhaustible means their energy. These nodes are the most important system design criteria for optimization energy conservation. The lack of energy in MANET mobile nodes causes the serious problem in the network. Nodes in MANET act as a both router and host.

D. Limited Physical Security

The mobile wireless networks are generally more prone to objective security threats than fixed-cable network .The increased possibility of eavesdropping, spoofing, denial-of service and intrusion attacks should be carefully measured .The security techniques are used to reduce security threats. The decentralized techniques provide additional control of robustness against the single points of failure of more centralized approaches.

E. Autonomous Terminal

ISSN: 2277-9655
Impact Factor: 1.852

The mobile terminal is autonomous node, which may function as similarly a host and a router. The host performs basic processing ability and the mobile nodes are able to perform switching functionality.

Security Issues in Manet

Security in MANET is a major issue as to provide secure communication between the nodes in the infrastructure less environment [5]. As ad hoc network is self organizing, open node to node connections, dynamic topology, and limited resources. A secure network is that which possess the following attribute:

A. Confidentiality

The confidentiality is to keep the information secret from the unwanted access. It is necessary to maintain the information safe and secure from the attacks.

B. Integrity of Message

It is used to keep the accuracy and consistency of the data during its transit from node to node. The data is not modified by the unwanted access.

C. Availability of Nodes

As in MANET for communication the nodes are needed to be available all the time so that the information can be relayed over such path.

D. Authorization

It specifies the privileges and the permissions of the entity participating in the communication over network.

Attacks in Manet

Securing mobile ad-hoc networks is a highly challenging issue [5]. Understanding probable form of attacks is always the first step towards developing superior security solutions. Many characteristics might be used to categorize attacks in the ad hoc networks.

External and Internal Attack

External attackers are primarily outside the networks who want to get access to the network and once they get access to the network they start sending bogus packets, denial of service attack in order to interrupt the performance of the whole network [2]. While in internal attack the attacker wants to have typical access to the network as well as contribute in the normal activities of the network. The attacker increase access within the network as new node also by compromising a current node in the network or by malicious imitation and start its malicious behaviour. Internal attack is more cruel attacks then external attacks.

Active and Passive Attack

Active attacks are able to do an internal or an external attack. The active attacks are intended to destroy the performance of network in such case the active attack act as internal node in the network [2]. Being a dynamic part of the network it is simple for the node to use and hijack any internal node to use it to introduce bogus packets injection or denial of service.

This attack brings the attacker in burly position where attacker can modify, fabricate and replay the massages. Attackers in passive attacks do not interrupt the normal operations of the network In Passive attack, the attacker listen in to network in order to obtain information, what is going on in the network. It listens to the network in order to identify and understand how the nodes are communicated with each other, how they are situated in the network. Before the attacker launch an attack beside the network, the attacker has sufficient information about the network that it can simply hijack and inject attack in the network.

Black Hole Attack in MANET

A packet drop attack or black hole attack is a type of denial-of-service attack in which a router that is supposed to relay packets instead discards them [2]. Black holes refer to places in the network where incoming traffic is silently discarded (or "dropped"), without informing the source that the data did not reach its intended recipients. Black Hole attacks effects the packet delivery and to reduce the routing information available to the other nodes causes: (i) It down grade the communication, (ii) Effects of making the destination node reach Black hole attack can be done by single malicious node is single black hole attack .A group of malicious node, which is known as cooperative black hole attack.

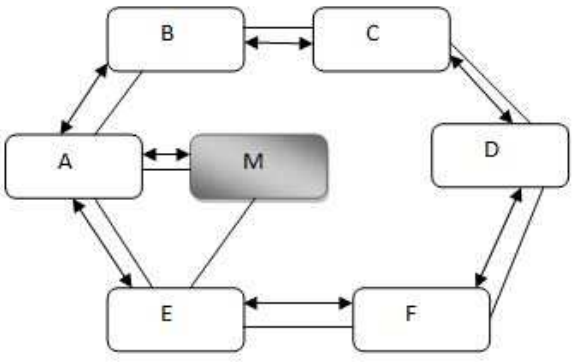

Figure 5.1 Single Black hole Attack

Black Hole Attack Detection Method

Security in MANET is a major problem to provide secure communication between the nodes. Detecting black hole attacks is not easier task. To handle this situation several approaches have been proposed. In this survey, 5 approaches are described in detail.

ISSN: 2277-9655
Impact Factor: 1.852

Black Hole Attack Detection Using a Probability of Attacks

In the Black Hole attack a node will participate in routing but will drop all the packets it receive [6]. The malicious node will always advertise in the network that it has a fresher route to the destination by setting the sequence number to a large value and will reply to the broadcast Route Request packet (RREQ) before other nodes send a reply. Thus the attacker node will attract all the traffic in its transmission range towards itself and then drop the packets.

First to determine the value of Black Hole, this ratio dropped to 3-10% from 90.Thus value of Pb (probability of Black Hole attack) =0.9. The value of threshold is taken as 10. That means the probability of attack is checked after sending out each 10 packets. Since the interval is given as 5 if the probability of attack (P*a*) goes above the threshold Pb=0.9 twice within 5 checks, a black hole attack is identified. The attack is identified and detected the source node will send a new Route Request and a new path will be established from source to destination.

Black Hole Attack Detection Using a Dynamic Data Routing Information

The Dynamic Routing Information table is used to counter black hole attack in MANETs. The Data Routing Information (DRI) table, which is used to identify the nodes of Cooperative black hole, it consists in adding two additional bits of information [8]. These bits have as values 0 for "FALSE" and 1 for "TRUE "for the intermediate nodes answering the RREQ of node source. Each node updates an additional table of information of the data routing.

Node	Data Routing Information	
	From	Through

Figure 5.2 Structure of DRI

The DRI table first bit from represents the information of the packet. The second bit through represents the information on the packet by node. To counter this attack, use data routing information table. This table stores two types of information- the node from which the packets comes and the node through which its forwards the packets.

The example the entry 1 and 0 for node A means “0” for node A means that the node B forwards the packets data coming from A but it doesn't forward any packet of data through node A. The entry “1, 1” for the node C means that the node B forwards the packets data coming from node C and the packets of data through C. This example is represented in the following table:

Node#	DRI	
B	From	Through
A	1	0
C	1	1

Table 1: Example of DRI Table utilization

Black Hole Attack Detection Based On Authentication Mechanism

The black hole attacks an authentication mechanism for identifying black hole nodes, which could be potentially exploited by malicious nodes [3]. It is constructed based on hash function. Time synchronization is imposed in the network so that each mobile node can synchronize the same time. A node partitions the whole time into equal intervals. The encryption and decryption methods are using the symmetric crypto system. Global symmetric key is used to encrypted the packet and send to the intermediate node.

The intermediate node is used forward the packet to next node. The decrypted the packet to destination node. Packet is valid packet the security routing is provided to source to destination node. Then the source node begins the data send to source node to destination node. Control Overhead routing control packets to detect the black hole attack. Transmissions are counted instead of packets since the goal is to compare data transmission to routing related transmissions. An authentication mechanism eliminates the need other forms of authentication infrastructure, which are usually not practical in MANETs.

Black Hole Attack Detection Using a Cryptographic Approach

Cryptography is the study of mathematical system concerned with protecting information or data from adversaries [4]. Cryptography provides security of information such as accessibility, validity data secrecy, Data integrity and Non repudiation. Also it makes available secure routing in MANETs. In this paper, a cryptographic approach has been proposed for secure routing to overcome black hole attack in MANETs.

The primitive functions of cryptography are symmetric key, Asymmetric key and Message Digest. The symmetric key cryptography one key is used both sender and receiver. Asymmetric key contains two key public and private key. The public key is defining encryption method. The private key is defined decryption method.

In this approach hop count is encrypted using famous well known RSA (Rivest Shamir Adelman) algorithm. Black hole attack arises in route discovery

ISSN: 2277-9655
Impact Factor: 1.852

phase. Essentially black hole attack is change of hop and immediate response using sequence number in the field of RREQ (Route Request). It involves three steps: Key Generation, Encryption and Decryption. The Encryption method the destination node sends the message public key to source node. The private key keeps the information secret then source node send the message to destination node. The decryption method the destination node recovers the original message. The attack node can be detected since the node encrypted the hop count and sequence number. The original message can be received using decrypt method.

Black Hole Attack Detection Based On Neighborhood Detection Method

In neighborhood-based method to detect the black hole attack and then present a routing recovery protocol to establish the path to the true destination such that the impact of the black hole attack can be mitigated [7]. The neighbor set of node is introduced in a metric. Neighbor set is clear as all the nodes that are radio transmission range of the node. Because of the mobility of nodes, the neighbor set of a node keep modifying and it is expected that the neighbor set changes faster when mobility increases. In order to collect neighbor set information, there introduce two types of control packets in the detection phase: Request Neighbor Set (RQNS) and Reply Neighbor Set (RPNS).

The first step was Collect neighbor set information. Determine whether there exists a black hole attack. The source node S, after receiving more than one RPNS packet in a certain period, will start comparing the received neighbor sets. The difference among the neighbor sets is defined as the union of the received neighbor sets minus the intersection of the neighbor sets. If the difference is larger than the predefined threshold value, S will know that the current network has black hole attacks and take some actions to detection process. The first destination node requests the neighbor set destination node. The neighbor set nodes reply the source node. The destination node claims the destination address. Destination address requests to neighbor sets. Destination neighbors can send urgent request to source node “D is masquerader node”. The drop the attack packet and alert the source node.

Conclusion

The Black hole attack is the primary security problem in ad hoc network .Black hole attacks are major attacks, probably that need to be addressed in mobile ad hoc networks. Many approaches are used to detect Black hole attack. In this paper, we have discussed five different approaches to moderate the security issues faced in MANET. In each method we have seen about how Black hole attacks are identified and detected and handled effectively by different methodologies that are employed.

References

[1] Carlos de Morais,P.Agrawal, “Mobile Ad hoc Networking”, 2003.
[2] Irshad Ullah , Shoaib Ur Rehman, “Analysis of Black Hole attack On MANETs Using different MANET Routing Protocols”, June 2010.
[3] Junhai Luo, Mingyu Fan, and Danxia Ye., “Black Hole Attack Prevention Based on Authentication mechanism”, 2008.
[4] Mohan Kumar S B, S Benni, “Cryptographic Approach to Overcome Black Hole Attack in MANETs”, International Journal of Innovations in Engineering and Technology Vol. 2 Issue 3 June 2013.
[5] Priyanka Goyal,Vinti Paramar,”MANET: Vulnerabilities, Challenges, Attacks, Application”, International Journal of Computational Engineering & Management, Vol. 11, January 2011.
[6] Shabir Sofi, Eshan Malik, Rayees Baba, Hilal Baba, Roohie Mir , “Analysis Of Byzantine Attacks In Ad hoc Networks And Their Mitigation”, 2012.
[7] Snigdha Arora, Rakesh Sharma, “Detection Of Black Hole Attack Using Neighborhood Set Based Method”, International Journal Of Research In Computer Engineering And Electronics. 1 ISSN 2319- 376X Vol : 1 Issue :2 October 2012.
[8] S.J. Sultanuddin, et al, “An Efficient Approach For Countering Black Hole Attack In Manets “,International Journal of Computer and Electronics Research [Volume 2, Issue 2, April 2013].