International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)
Web Site: www.ijettcs.org Email: editor@ijettcs.org
Volume 4, Issue 6, November - December 2015 ISSN 2278-6856

A Survey on Detection and Prevention of Black Hole Attack in MANET

Shridevi.K [1], Sudha.S[2]

[1] Department of Computer Science and Engineering,
Secab Institute of Engineering & Technology, Vijayapur, Karnataka, India

[2] Department of Computer Science and Engineering,
Secab Institute of Engineering & Technology, Vijayapur, Karnataka, India

Abstract

Mobile adhoc network (MANET) is a collection of wireless mobile nodes and use the wireless connections to connect to the various networks. It doesn't require any base station. Mantes are prone to various kinds of security attacks as black hole, worm hole, gray hole and Man in middle attack. Possible and common attack in adhoc network is black hole attack. In black hole attack malicious node provides fake routing information by advertising itself as having shortest path to destination and then drops the packets later. In this work the survey is considered on the various methods to detect and prevent black hole attack in MANET.

Keywords: MANET; Black hole; AODV; DSR

1. INTRODUCTION

A MANET contains wireless mobile nodes which have the ability to communicate with each other without having fixed infrastructure. MANET is a type of adhoc network that can change locations and configure itself. So every node in network acts as source and route packets to other nodes in network.

MANET Characteristics:

- Dynamically changing network topology
- Lack of centralized monitoring
- Cooperative algorithms
- Bandwidth constraint
- Limited physical security
- Energy constrained operation

Security attributes of MANET:

In providing Secure networking environment some of services may be required. To secure an adhoc environment, considering the following parameters such as the

- Authentication
- Confidentiality
- Integrity
- Availability
- Authorization
- Non repudiation

The paper is organized as follows. Section 2 provides an overview of AODV protocol and DSR protocol, some of the attacks performed in MANET, section 3 deals with several methodologies to detect and prevent black hole attack, section 4 presents a comparison table among the solutions and finally conclude the paper in Section 5.

2. OVERVIEW OF AODV PROTOCOL

Ad-hoc On-Demand Distance Vector (AODV) is an on demand routing protocol, which is used to find a route between the source and destination node as needed. The mobile devices or nodes in the network exchange the routing packets between them when they want to communicate with each other and maintain only these established routes.

The basic message set consists of RREQ – Route request, RREP – Route reply, RERR – Route error. Whenever source wants to communicate with destination it sends RREQ. Destination or intermediate node sends back reply to RREP to message to source. If there is breakage in link between nodes it sends RERR message to source node that it has lost link. Hello message is used for detecting and monitoring links to neighbors.

3. OVERVIEW OF DSR PROTOCOL

The DSR is a simple and efficient protocol for routing in mobile, ad hoc and wireless networks. DSR is suitable for routing in multi-hop networks. A mobile ad hoc network is completely self organizing while using the DSR protocol. All nodes cooperate to forward packets. Nodes in the network may move about, join or leave. All routing is automatically determined by the protocol. The number and sequence of intermediate hops needed to reach any destination may change dynamically. Hence the network topology may be quite complex. DSR is an on-demand or reactive routing protocol. When a source node S wants to send a message to a destination node D, the process starts with a route discovery phase. The message is sent once a route has been discovered and S knows about the discovered route. However, DSR extensively takes advantage of existing knowledge of the network topology. Each node gathers information about the network topology by overhearing other nodes' transmissions. This is known as promiscuous mode of operation. Each node maintains a route cache to remember routes that it has learnt about. One of the main advantages of DSR as opposed to a table driven protocol like DSDV is that the number of control messages is much smaller. Hence DSR is more energy-

efficient and does not congest the network with too many control messages.

Table 1: Attacks on MANET

Type of Attack	Description
Black hole	Drops the packets by sending false route reply messages to the route request instead of forwarding.
Wormhole	Tunneling the packets in one location of network and receiving packets in other location of network. Tunneling between two colliding attackers in the network.
Gray hole	Nodes can drop the packets partially and act as honest node.
Man in middle	Messages between two parties who believe they are communicating directly with each other. Fact is that controlled by an attacker itself.
Byzantine	Selectively drop packets by making routing loops, forwarding packets through non-optimal paths with compromised nodes.
Rushing	Quickly forwards the control messages to gain the access to the network .On demand routing protocols that use the duplicate suppression during route discovery process which are vulnerable to this attack.
Resource consumption	Malicious node tries to consume, waste resources of other nodes present in the network.
Information disclosure	Compromised node may leak confidential or important information to unauthorized nodes in the network.

4. METHODOLOGIES TO DETECT AND PREVENT BLACK HOLE ATTACK

Latha Tamilselvan, V Sankaranarayanan [1], presents a solution that modifies the AODV routing protocol, which avoids the multiple black holes nodes in the network. It uses the Fidelity table that where the participating node in the network is assigned a fidelity level that gives the reliability for that node. If the level of node is 0 values, it is considered as a black hole node and it will discarded from the network. Solution for detection of Black hole is that before sending data packets to the route ensure about the reliability of it.

Tamilselvan L et al. And V. Sankaranarayanan [2], proposes a solution based on an AODV routing protocol. The source node has to wait for other replies with next hop information without sending the data packets to the destination. The concept is setting timer for collecting the other request from other nodes after receiving the first request. It sets timer in the Timer expired table, to collect the further RREP from different nodes are stored in Collect route reply table (CRRT) with the sequence number, and the time at which the packet arrives. The route validity is checked based on the arrival time of the first request and the threshold value.

Deng et. al. [3], has proposes an algorithm to prevent black hole attacks in ad hoc networks. According to their algorithm, any node on receiving a RREP packet, it will cross checks with the next hop on the route to the destination from a correct path. If the next hop either does not have a link to the node that sent the RREP or does not have a route to the destination then the node that sent the RREP is considered as malicious. This technique does not work when the malicious nodes cooperate with each other. In this when any intermediate node replies for RREQ, it includes the next hop information to the destination in the RREP packet. When the source node receives this RREP packet, it sends a further request to the next hop of the replied node and asks them about the replied node and about the route to the destination. Thus easily identify of the replied node if the next hop is trusted otherwise not.

Fidel Thachil, K C Shet [4], proposes a trust based approach for AODV protocol to mitigate black hole attack in Manet. The black hole attack can interrupt the communication between the various nodes in AODV for MANET. In the AODV the malicious activities are not monitored. AODV is most widely used protocol for Manet. In case of AODV all mobile nodes work in cooperation to find a route path from source to destination. Data transmission will take place only after the route is established. AODV uses the three control messages. These messages are RREP, RREQ and RERR. Here each node monitors the neighboring node and calculates the trust value of the neighboring node. If the trust value of a monitored node goes below a threshold, then the monitoring node assume it as malicious and avoids that node from the route path.

Mohanapriya and Krishnamurthy [5], presented a Modified Dynamic Source Routing Protocol (MDSR) to detect and prevent selective black hole attack. The source node selects the first shortest path to the destination, to intimate the no. of data packets it sends to the destination. The source node then selects the second shortest path for actual transmission of data. Then packet count and transmitted data both are compared. If difference is significant i.e. abnormality is detected the nearby IDS node broadcast a message informing all nodes to obscure all nodes from network.

Prachee N. Patil, Ashish T. Bhole [6], and Black Hole Attack Prevention in Mobile Ad Hoc Networks using Route Caching: The Dynamic Source Routing (DSR) algorithm makes use of caching concepts to store all newly constructed routing paths in mobile ad hoc networks. Route caching is aggressively used by DSR. By virtue of source routing, it is possible to cache every overhead route without causing loops. Basically the

forwarding nodes are caching source route from the packet and forwards it for future use. Also, the destination replies to all requests. Thus the source learns many alternate routes to the destination that are cached. In this paper author propose a new approach for black hole prevention in DSR based on route caching. In this approach, once the black hole node is detected in MANET during the path construction, pass the black hole node id to path function of DSR. In this function, paths are ready to be added in route cache; however priory to add each path in route cache is decided by passing these paths for presence of black hole node id.This process makes use of normal time of Caching process only.

Anita et al. [7], proposed a mechanism for detecting black hole attacks in MANETs using a certificate based authentication method that can counter the eject of black hole Attack. They used certificate chaining for authenticating the nodes in the MANET. Their Solution consists of two phases: certificate phase and authentication phase. Once the route has been established between the source and destination nodes, the nodes forming the route enter into the Certitification phase. The source node then identifies the next hop node and generates the public key then issues the public key certificate to the node that the source node is convinced of having the security parameters. The issued certificates have an expiry time, considered as a certain time interval. The source node transmits the data to the destination node only if it receives the authenticated reply from the destination node. If the binding between the node and its key is found to be invalid, the issuing node revokes the certificate, and the node is considered to be malicious.

G. Indirani et al. [8], proposed a defense mechanism based on DSR algorithm having two extensions Watchdog and Pathrater. Watchdog module identify the misbehaving node by keeping a watch on node that it forward the packet to next node, if node does not forward the packet then it is considered as misbehaving node and is reported. Pathrater uses this information given by watchdog module and deletes the corresponding route from the route table and determine another route available to the destination by looking in its cache table. If no route available then Pathrater will broadcast a Route Request to get a new route to the destination.

Sangheetaa Sukumran et al. [9], proposed a solution for on-demand routing protocol using reputation mechanism. This approach calculates the reputation values of the nodes using simple formula. Any node is supposed to maintain a good reputation value in order to receive network services.. When a node tries to identify a route, its route request will be forwarded by the neighboring nodes only if it reputation value is higher than the threshold value i.e. this node must be in the white list. Thus a node needs to maintain a good reputation value in order to enjoy network services. A misbehaving node which is isolated has no chance of rejoining the network until the entire network is reformed. This will decrease the efficiency and effectiveness of the network, low reputation value node is not allowed to participate in a network until network is reformed. Provided a solution that uses reputation with cache clearance process that not only improve the efficiency and reduce network overhead but also permit every node to participate into the route selection process for communication.

Tsou, Chang, Lin, Chao and Chen [10], presented a novel approach entitled Bait DSR (BDSR) scheme to defend the collaborative black hole attacks. This approach has been composed of both proactive and reactive method to create a hybrid routing protocol. The basis routing protocol utilized is the Dynamic Source Routing on demand routing. In this approach, firstly the source node sends bait RREQ packet. A similar technique that was used in DSR is used here to prevent the traffic jam problem which will be generated by bait RREQ. These sent bait RREQs could easily detect malicious nodes and defend against black hole attacks. RREPs additional field is able to keep the identity of malicious nodes. Therefore, the source node could simply discover the situation of malicious nodes and Remove all the RREPs coming from that location. This approach has higher PDR in compare with existing DSR and the communication overhead was improved when compared with DSR routing protocol.

Vaishali B [11], proposed a modified DSR for mitigating Black hole Impact in MANET was proposed. In this approach a source node uses RREP available in its route cache or sent by an intermediate node for forwarding the first data packet and waits for the acknowledgment (ack).If ack comes within a certain time, then this route is safe and succeeding packets are sent on the same route otherwise to identify the presence of malicious node a fictive route request is sent along the suspected route with the destination address as fictive address which is not there in the network. The node that replies to this fictive route request is listed as black hole and it is not included in the further routing process. If the route reply is from destination node then the route is considered as safe route.

5. COMPARISON OF SOLUTIONS TO BLACK HOLE ATTACK

The various solutions to black hole attacks proposed by several authors are analyzed and made a comparison based on important parameters and depicted in Table2.

Table 2: Comparison of Solutions to Black Hole Attack

Author	Title	Methodology	Routing Protocol	Drawback
LathaTamilselvan, Dr.V.Sankaranarayanan	Prevention of Black hole Attack in MANET	Collect Route Reply Table(CRRT)	AODV	Delay
Latha Tamilselvan, Dr.V.Sankaranarayanan	Prevention of co-operative black hole attack in MANET	Fidelity table	AODV	Delay
Deng et.al	Simulation to detect and removal of blackhole attack in MANET	Route request and reply to next hop node	AODV	Routing overhead and black hole attack
Fidel Thachil, K C Shet	A trust based approach for AODV protocol to mitigate black hole attack in MANET	Trust based approach	AODV	
M. Mohanapriya and Ilango Krishnamurthy	Modified DSR protocol for detection and removal of selective black hole attack in MANET	MDSR for shortest path	DSR	Detection.
Prachee N. Patil , Ashish T. Bhole	Black Hole Attack Prevention in Mobile Ad Hoc Networks using Route Caching	Caching concept	DSR	Caching process
E. A. M. Anita	Black hole attack prevention in multicast routing protocols for mobile ad hoc networks using certificate chaining	Certificate based authentication method	DSR	The issuing node revokes the certificate.
G. Indirani, Dr. K. Selvakumar, V. Sivagamasundari	Intrusion Detection and Defense Mechanism for Packet Replication Attack over MANET Using Swarm Intelligence	DSR algorithm having two extensions Watchdog and Path rater	DSR	Fails to detect malicious nodes.

Sangheetaa Sukumran	Reputation based Dynamic Source Routing Protocol for MANET	Reputation method	DSR	
P.-C. Tsou, J.-M. Chang, Y.-H. Lin, H.-C. Chao and J.-L. Chen	Developing a BDSR scheme to avoid black hole attack based on proactive and reactive architecture in MANET	BDSR Scheme	DSR	
Vaishali B. Mewada, Viral Borisagar	Modified DSR for Mitigating Black hole Impact in MANET	routing is based on *DSR* with *modification*	DSR	

6. CONCLUSION

This paper lists out various works carried out to detect and prevent Black hole attack in MANET either using AODV protocol or DSR protocol. There are many advantages and disadvantages associated with each method such as time delay, control overhead and security. There is no fixed reliable procedure to detect and prevent black hole attack.

REFERENCES

[1]. Latha Tamilselvan and Dr. V Sankaranarayanan, "Prevention of Blackhole Attack in MANET", the 2nd International Conference on Wireless Broadband and Ultra Wideband Communications, pp. 21-26, 2007.

[2]. Latha Tamilselvan, Dr.V. Sankaranarayanan, "Prevention of Co-operative Black Hole Attack in MANET", Journal of Networks, Vol 3, No 5, 13-20, May 2008.

[3]. Deng et.al, "Simulation to detect and removal of blackhole attack in manet", 2015.

[4]. Fidel Thachil, K C Shet, "A trust based approach for AODV protocol to mitigate black hole attack in MANET", 978-0-7695-4817-3/12 $26.00 © 2012 IEEE DOI 10.1109/ICCS.2012.7

[5]. Mohanapriya, M. and Krishnamurthi L., "Modified DSR protocol for detection and removal of selective black hole attack in MANET", International Journal on computers and electrical engineering, Vol. 40, No. 2, pp. 530-538, 2014.

[6]. Prachee N. Patil , Ashish T. Bhole, "Black Hole Attack Prevention in Mobile Ad Hoc networks using Route Caching" ,2013.

[7]. Anita, E. M., & Vasudevan, V., "Black Hole Attack Prevention in Multicast Routing protocols for Mobile Ad hoc networks using Certificate Chaining", International Journal of Computer Applications, 1(12), 21-2, 2010.

[8]. G. Indirani, Dr. K. Selvakumar, V. Sivagamasundari, "Intrusion Detection and Defense Mechanism for Packet Replication Attack over MANET Using Swarm Intelligence", Pattern Recognition, Informatics and Mobile Engineering (PRIME) February 21-22, pp. 152-156, 2013.

[9]. Sangheetaa Sukumran, Venkatesh Jaganathan, Arun Korath, "Reputation based Dynamic Source Routing Protocol for MANET", International Journal of Computer Applications (0975 – 888) Vol.47, No.4, June 2012.

[10]. P.-C. Tsou, J.-M. Chang, Y.-H. Lin, H.-C. Chao and J.-L. Chen, "Developing a BDSR scheme to avoid black hole attack based on proactive and reactive architecture in MANETs", Proceedings of 13th International Conference on Advanced Communication Technology (ICACT), (Phoenix Park Gangwon-Do, Korea (South)), pp. 755 -760, Febraury 2011.

[11]. Vaishali B. Mewada, Viral Boris agar, "Modified DSR for Mitigating Black hole Impact in MANET", International Journal for Technological Research in Engineering Volume 1, Issue 9, May-2014 ISSN Online: 2347 - 4718.