International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 02 Issue: 09 | Dec-2015 www.irjet.net p-ISSN: 2395-0072

A Survey on Preventing DSR Protocol against Black Hole Attack for MANET

Rahul Patel, Maitrey Patel

Student, Dept. Of Computer Engineering, Grow More Faculty of Engineering Himatnagar, Gujarat, India
Asst. Professor, Dept. of Computer Engineering, Grow More Faculty of Engineering Himatnagar, Gujarat, India

Abstract- ***Now a day, Ad-hoc network has become an indivisible part for communication for mobile devices. A mobile ad hoc network (MANET) is a collection of wireless mobile nodes dynamically forming a network topology without the use of any existing network infrastructure or centralized administration. A black hole attack is a severe attack that can be easily employed against data routing in MANETs. A black hole is a malicious node that can falsely Reply for any route requests without having an active route to a specified destination and drops all the receiving data Packets. The Black hole attack is that where a malicious node advertises itself as it is having the optimal route to the destination. This paper discusses some of the techniques put forwarded by researchers to detect and prevent Black hole attack in MANET using DSR protocol.***

Keywords*: Mobile ad hoc networks, Security Attacks, Black hole attack, Dynamic Source Routing (DSR).*

1. INTRODUCTION

MOBILE ad hoc network (*MANET*) [1] consists of a many of wireless mobile nodes communicating with each other without any centralized control or fixed network infrastructure the wireless network can be classified into two types:

- Infrastructure network
- Infrastructure less or Ad Hoc network.

Every node has the self-configuring ability. Because every node has to act as both host and router, security problems are there in mobile ad hoc network. Every Node has the responsibility of forwarding the packets received by it.

There are various types of attacks that can occur in such type of network, so it is essential to detect such kind of attack and derive methods to exclude the malicious or misbehaving nodes and enhance the nodes cooperation.

In this paper, the famous denial of service attack, Black hole attack, is discussed. In this attack, malicious node behaves like a black hole and absorbs all the packets received by it.There should be mechanisms to detect and remove such nodes from the network for successful and errorless transmission of data. In this paper, various techniques to identify and remove of such black hole nodes are presented.

2. SECURITY ATTACKS [2], [3]

Attacks in MANET can be categorized into two parts:

- Passive attacks and
- Active attacks

A **passive attack** does not disturb the routing protocol operation, but only tries to find valuable information by listening to routing traffic, so it is very difficult to detect.

An **active attack** is an effort to alter the data, authentication gain, or procure authorization by inserting false packets into the data stream or modifying packets transition through the network.

Active attack can be further divided into external attacks and internal attacks.

An **external attack** is one in which participating nodes are not part of the network

An **internal attack** is one in which compromised or malicious nodes are part of the network.

Different types of **Network Layer attacks** are described below [2]:

1). Black Hole Attack: In this attack, malicious nodes absorb the packets received by it without forwarding to the next hop. It can either use the packet information for wrong purpose or discard the packets.

2). Wormhole Attack: In this attack, a malicious node receives packets from one location in the network and tunnels them to another location in the network, where these packets are again sent into the network. This tunnel between two conspiring attackers is referred to as a wormhole.

3). Byzantine Attack: A malicious intermediate node works alone, or a set of malicious intermediate nodes works in

mutual agreement. Examples of such attacks are creating routing loops, forwarding packets using fake paths, or selectively dropping packets, which results in the degradation of the routing services and poor network performance.

4). Sleep Deprivation Attack : This kind of Attack run out of limited resources, like battery powers, in the mobile ad hoc nodes, by constantly making them busy processing unnecessary packets. In a routing protocol, sleep deprivation attacks might be caused by flooding the targeted node with unnecessary routing packets.

5). Location Disclosure: In this attack, attacker reveals information regarding the location of nodes or structure of the network. It collects the various node location information and plans the further attacks.

6). Eavesdropping: The purpose of this attack is to eavesdrop the secret information passing to the network. This Confidential information can be location of the nodes, passwords, public-private keys also.

7). Flooding: In this attack, Networks are flooded by fake RREQ and data packets which create the congestion in the network and make it difficult for the network to transmit the information to actual destination nodes.

3. OVERVIEW OF DSR PROTOCOL [4]

One of the most popular on-demand routing protocol is dynamic source routing protocol (DSR) in which a node attempts to discover a route to some destination only when it has a packet to send to that destination. DSR consists of two phase: route discovery and route maintenance. Route Discovery is the process of finding the route from one node to another i.e. source to destination,

A. Route Discovery

Route Discovery is divided into two stages: Route Request (RREQ) and Route Reply (RREP). Whenever a node wants to communicate in the network and does not have a route in its Route Cache to the destination, it broadcasts a RREQ message to get a route.
This process continues until either the maximum hop counter is reached or the destination is reached. When the destination node receives the RREQ packet, appends its address and generates a route reply packet (RREP) and send towards the source using the reverse of the list of the nodes in RREQ.
When the source node receives RREP, it first stores the route in its Route Cache and then sends data packets through that route.

B. Route Maintenance

In **Route Maintenance** phase, when data is being transmitted and an intermediate node detects that the network topology has changed or the data can't be transmitted to its next hop, it generates a route error packet indicating that the next hop is unreachable; it also appends its own address in the packet and send it towards the source node.

4. BLACK HOLE ATTACK [3], [5], [6]

MANETS are vulnerable to various types of attacks. On the basis of different characteristics the attack on mobile ad hoc network is classified as passive and active attacks.
The Black hole attack is an active insider attack.
One such active attack is Black hole attack. A black hole is a node that has the characteristics that it always responds with a RREP message to every RREQ, even though it does not really have a legitimate route to the target node.

4.1 Types of Black Hole Attacks

A Black Hole attack is a type of denial of service attack wherever a malicious node be able to be a focus for all packets by incorrectly claiming a new route to the destination and after that attract them without forwarding them in the direction of the destination.

Single Black Hole Attack

In single black hole attack only one malicious node attack on the route. See fig.1

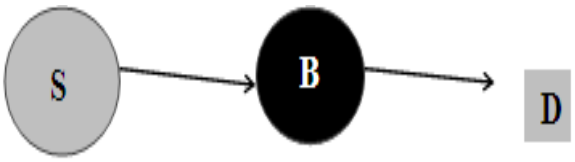

Fig. 1 Single Black Hole Attack [3]

Co-operative Black Hole Attack

In the Co-operative Black Hole attack the malicious nodes have an effect in a group. The nodes 2 and 3 act as black holes. See fig.2

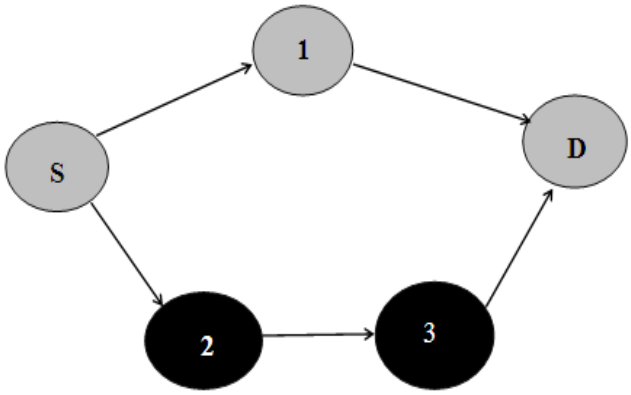

Fig. 2 Co- Operative Black Hole Attack[3]

During the Route Discovery process, the source node sends RREQ packets to the intermediate nodes to find fresh path to the intended destination.
Malicious nodes respond immediately to the source node as these nodes do not refer the routing table. The source node assumes that the route discovery process is complete, ignores other RREP messages from other nodes and selects the path through the malicious node to route the data packets. The malicious node does this by assigning a high sequence number to the reply packet. The attacker now drops the received messages instead of relaying them as the protocol requires.

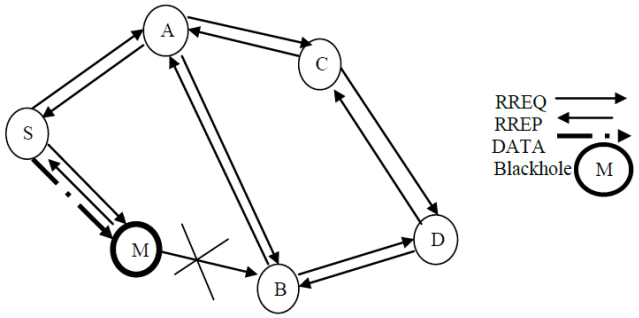

Fig. 3 Black hole Attack[6]

In the above fig. 3, imagine a malicious node M. When node A Broadcasts a RREQ packet, nodes B, D and M Receive it. Node M being a malicious node, does not check up with its routing table for the requested route to node E. Hence, it immediately sends back a RREP packet, claiming a route to the destination. Node A receives the RREP from M ahead of the RREP from B and D. Node A assumes that the route through M is the shortest route and sends any packet to the destination through it. When the node A sends data to M, it absorbs all the data and thus behaves like a Black hole.

5. LITERATURE REVIEW

In [6], The DBA-DSR scheme is designed to identify and isolate the black hole nodes present in the MANET. This protocol is a modified version of DSR, in which fake RREQ packets are used to identify the malicious nodes.

In [7], proposed a DSR based secure routing protocol called Baited-Black-hole DSR (BDSR) that can detect and avoid black hole attacks in MANETs. In their approach, the source node stochastically selects an adjacent Node with which to cooperate, in the sense that the address of this node will be used (as the bait destination address) to bait malicious nodes to reply to the RREP message.

In [8], Jain et al. introduced an algorithm for detecting and removing black hole attacks in MANETs. Their technique consisted in sending equal and small sized blocks of data and monitoring the flow of these data blocks independently at the neighborhood of both the source and destination nodes, with the goal to detect a chain of cooperative malicious nodes can be detected.

In [9], Anita et al. proposed a mechanism for detecting black hole attacks in MANETs using a certificate based Authentication method that can counter the effect of black hole attack.

In [10], Weerasinghe and Fu proposed a solution for prevention cooperative black hole attacks in MANETs. In their solution, each node maintains a table called Data Routing Information (DRI), which is used to identify the misbehaving nodes in the network. The DRI table uses 0, 1 to keep track of whether or not a node has transferred the data to its neighbor's.

In [11], proposed a solution to avoid the black hole attack in MANETs. According to their solution, each intermediate node should include the information of the next hop to destination in its route reply (RREP) packet when the intermediate node replies to the route request (RREQ) packet.

In [12], Association based Routing which is to be applied over the DSR protocol in order to enhance the security. The purpose of this scheme is to fortify the existing implementation by selecting the best and secured route in the network.

In [13], Intrusion Detection Systems (IDS) are one of the main techniques utilized to prevent attacks against security threats. Intrusion detection is a process of

detecting an adversary and preventing its subsequent actions.

In [14], ABDSR routing protocol, which will be able to evade cooperative black holes.ABDSR approach involves that all nodes participate in communication and to fight against the Black hole attack is to make use of a "Reputation Table" where in every participating node will be assigned a reputation level that acts as a measure of trustworthiness of that node.

In [15], Public Key Infrastructure (PKI)is one of the most effective tools for providing security for dynamic networks.. The Proposed scheme uses the route discovery scheme of DSR to issue security certificates.

In [16] performed a work," Detecting Black hole Attacks on DSR-based Mobile Ad Hoc Networks". In this paper, a novel scheme for Detecting Black hole Attacks in MANETs (so-called DBA-DSR) is introduced. The BDA-DSR protocol detects and avoids the black hole problem before the actual routing mechanism is started by using fake RREQ packets to catch the malicious nodes.

6. CONCLUSION

This paper mainly focused on the black hole attack in network. How it is detect from the network .How can we prevent our data from malicious node. In this paper a survey on different existing techniques for detection of black hole attacks in MANETs with their defects is presented. The detection techniques which make use of proactive routing protocol have better packet delivery ratio and correct detection probability, but have higher overheads.

REFERENCES

[1] S. Corson and J. Macker, "Mobile ad hoc networking (MANET): Routing protocol performance issues and evaluation considerations," IETF RFC 2501, Jan. 1999.

[2] Vaishali B.Mewada,Viral Borisagar,"MODIFIED DSR FOR MITIGATING BLACKHOLE IMPACT IN MANET",International Journal For Technological Research In Engineering Volume 1, Issue 9, May-2014

[3] Gurnam Singh, Gursewak Singh,"Improvement of Network Efficiency by Preventing Black Hole Attack in Manet",International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume 4 Issue-2, July 2014

[4] D. B. Johnson and D. A. Maltz, "Dynamic Source Routing in Ad Hoc Networks", Mobile Computing, T. Imielinski and H. Korth, Eds., Kulwer Publ., 1996, pp. 152-81.

[5] Ashish T. Bhole, Prachee N. Patil, "Study of blackhole attack in MANET", International Journal of Engineering and Innovative Technology (IJEIT) Volume 2, Issue 4, October 2012

[6] ChanderDiwaker,Sunita choudhary,"DETECTION OF BLACKHOLE ATTACK IN DSR BASED MANET",International Journal of Software and Web Sciences (IJSWS),www.iasir.net

[7] P-C Tsou, C. J-M Chang, Y-H Lin, H-C Chao, J-L Chen,"Developing a BDSR Scheme to Avoid Black Hole Attack Based on Proactive and Reactive Architecture in MANETs", ICACT 2011,. Feb. 13~16, Phoenix Park, Korea, 2011,

[8] S. Jain, M. Jain, H. Kandwal, "Advanced Algorithm for Detection and Prevention of Cooperative Black and Grayhole Attacks in Mobile Ad Hoc Networks", Intl. Journal of Computer Applications 1(7):37–42, Feb. 2010.

[9] E. A .M. Anita, V. Vasudevan, "Blackhole Attack Prevention in Multicast Routing Protocols for Mobile Ad hoc networks using Certificate Chaining", Intl. Journal of Computer Applications, vol. 1, No. 12, 2010.

[10] H. Weerasinghe, H. Fu, "Preventing cooperative black hole attacks in mobile ad hoc networks: Simulation implementation and evaluation", Proc. of Intl.Conference on Future Generation Communication and Networking (FGCN'07), Jeju Island, Korea, pp. 362-367, 2007.

[11] N.Bhalaji, Dr.A.Shanmugam,"ASSOCIATION BETWEEN NODES TO COMBAT BLACKHOLE ATTACK IN DSR BASED MANET",978-1-4244-3474-9/09/$25.00 ©2009 IEEE.

[12] IsaacWoungang, SanjayKumar ,Rajender DheerajPeddi,andMohammad S.Obaidat,"Detecting Blackhole Attacks on DSR-based Mobile Ad Hoc Networks",978-1-4673-1550-0/12/$31.00 ©2012 IEEE

[13] Yibeltal Fantahun Alem,Zhao Cheng Xuan,"Preventing Black Hole Attack in Mobile Ad-hoc Networks Using Anomaly Detection",978-1-4244-5824-0/$26.00 c 2010 IEEE

[14] Shinni Mittal,Harish Taluja,"Analysis of Cooperative Black Hole Attack Using Dynamic Source Protocol",International Journal of Advanced Research in Computer Science and Software Engineering,Volume 2, Issue 8, August 2012.

[15] K.Selvavinayaki K.K.Shyam Shankar Dr.E.Karthikeyan,"Security Enhanced DSR Protocol to Prevent Black Hole Attacks in MANETs",International Journal of Computer Applications (0975 – 8887) Volume 7– No.11, October 2010

[16] Isaac Woungang," Detecting Blackhole Attacks on DSR-based Mobile Ad Hoc Networks", 978-1-4673-1550-0/12©2012 IEEE