Efficient Security Approaches to detect Blackhole Attack in Wireless Network: A survey

[1]Gouri Upadhyay, [2]Aditya Kumar
[1]M.Tech. Scholar, [2]Assistant Professor
[1]Computer Science & IT Department,
[1]Shri Shanakara Charya Engineering College, Bhilai, Chhattisgarh, India.

Abstract: This Wireless networks are decentralized and the infrastructure less networks, where nodes at any given moment can join or leave the network. Because ad hoc networks are autonomous mobile nodes, they form a temporary network that does not have a fixed infrastructure. Each node in the network is autonomous; therefore, they act as hosts and as routers. Because of this nature of MANET, where any node can join or leave the network without authorization, security is the main challenge in these networks. One of the main security problems of MANET is the attack on the black hole. It happens when a malicious node called a black hole joins the network, during the path discovery process, this node acts as if it had the path to the destination and takes all the packets and does not forward to the desired destination. In this paper, a survey is presented on some of the techniques and methodologies for detecting and preventing black hole attacks in wireless networks and a table representing their advantages and disadvantages.

Index Terms **- MANET, AODV Routing Protocol, Ad hoc network, Black hole**

I. INTRODUCTION

The ad hoc wireless networks are a group of autonomous nodes that can self-manage without infrastructure. MANETs are spontaneous and dynamic, so any node can join or leave the network at any time. Because of this, they are widely used in military and rescue areas where communication between soldiers on the battlefield and in areas where a new temporary network is required because the network could collapse due to some disaster. Ad hoc networks are temporary networks established in a place where no fixed infrastructure is required.

The nodes act as hosts and routers that exchange and forward packets for communication. MANET uses routing protocols for such communication can be proactive routing protocols (direct table routing protocol) in which the routing information of the nodes is routinely exchanged vector distance sequenced routing protocol DSDV destination link state optimized by OLSR. Or the reactive routing protocol (on-demand routing protocol) in which the route is established and the nodes exchange information only when necessary, such as the ad hoc AODV distance vector, the dynamic source DSR.

In addition to acting as host nodes they also act as routers to discover nodes and forward packets to the correct node on the network. Because ad hoc wireless networks do not have a fixed infrastructure, they are more open to attack. One of the main attacks is the attack of the black hole. In which the evil knot absorbs all the packets in it like a hole that sucks everything, the so-called black hole attacks.

In the AODV routing protocol, the path discovery process is performed by the intermediate nodes responsible for finding a new route to the destination by sending detection packets to the adjacent nodes. The malicious node does not follow this process, but responds immediately to the input node with false information indicating that it has the new path to the destination. The source node then sends all its packets to the destination through this malicious node, assuming it has the value. Black hole attack occurs when the malicious node discards all packets and sends packets to the desired destination node.

II. CLASSIFICATION OF ATTACK

Based on the source of the attacks [1]:
1. External attack: the external attack occurs due to nodes that are not part of the network.
2. Internal attack: the internal attack occurs through the nodes belonging to the network (compromised nodes).

Based on the behavior of attacks [1]:
1. Passive attacks: they obtain information from the exchange of data in the network, but do not cause any modification of the data or do not interrupt the communication in progress [2].
2. Active attacks: get information from the exchange of data in the network and modify the data or interrupt the communication in progress [2].

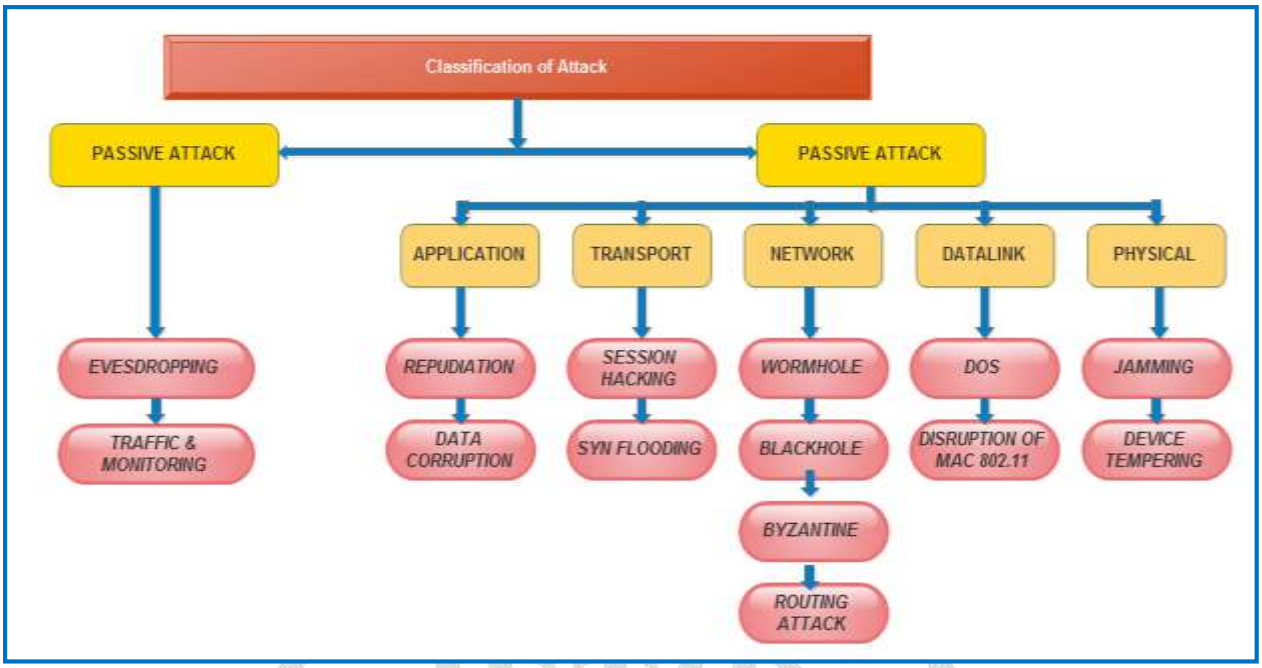

Figure 1: Classification of Attacks

III. BLACK HOLE ATTACK

It's a very serious attack on MANET. In Blackhole Attack, an unpleasant node transmits the entire neighboring node that has the smallest path to the destination node without looking at its routing table. Source will send your data to this malicious node. And after having obtained all the data, it is not forwarded to the destination, but all data is deleted [3].

Figure 3 explains how the black hole problem occurs. Node A sends data to node D and begins the process of finding the path. Send RREQ message to all adjacent nodes. Node C is an unpleasant node and declares that it has the smallest path to the destination node. Then it will send the RREP message to node A. Node A will assume that this is the shortest way and will ignore all other answers. When node C receives all data packets, it compresses all data. Thus, an unpleasant node attracts all network traffic to itself, announcing that it has the smallest path to the destination node, hence the loss of data in the network.

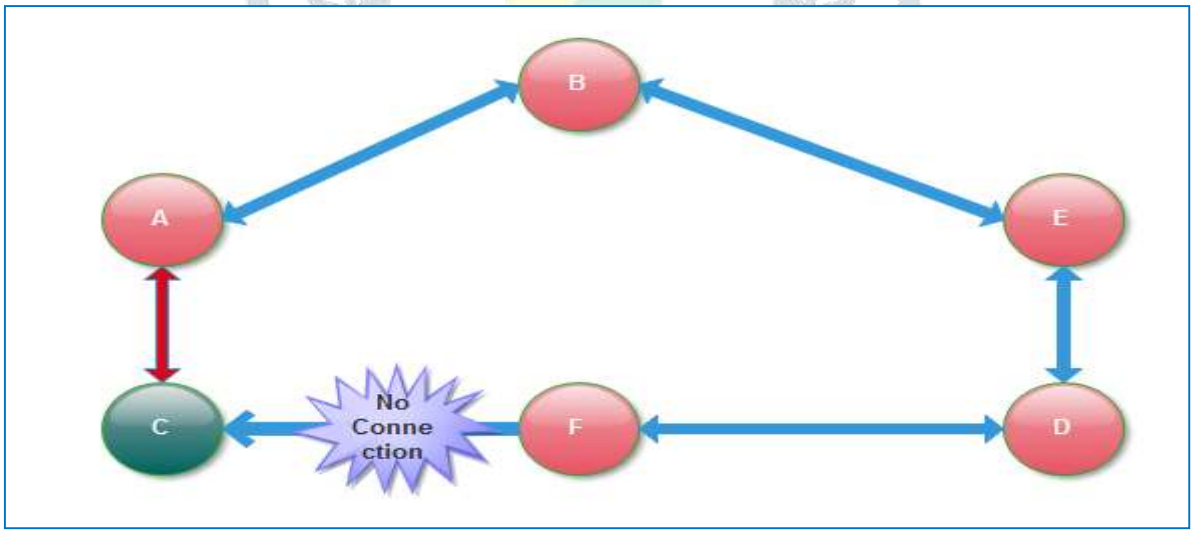

Figure 2: Black hole Problem

In AODV, we can classify a black hole attack [1] in two types:

(i) Internal attack of the black hole:

In this type of attack, an unpleasant inner knot is inserted between the sender and the receiver. Once it has a chance, the unpleasant knot becomes an authorized knot. Subsequently, it may disturb the communication in progress of the network.

(ii) External attack of the black hole:

An external attack actually remains outside the network and refuses access to network traffic or creates bottlenecks in the network or interrupts the operation of the entire network. It can become an internal attack when it takes control of the unpleasant internal node and manages it to hit other nodes in the network area.

A. Attack of a single black hole:

In the attack of a single black hole, there is only one malicious node in an area. The other nodes will be an authorized node [4]. As shown in Figure 3. Node A is the initial node and Node D is the final node. Node C is a malicious node and responds to the RREQ packet sent by the initial node A and erroneously answers that it has the smallest path to the final node. Therefore, node A believes that the path discovery process has been completed and starts sending data packets to node C. In MANET, a malicious node removes all data packets. This problem is known as the black hole problem in MANET.

B. Collaborative attack of the black hole:

In this black hole attack, more than one malicious node is present in the network. It is also known as Black Hole Attack with harmful nodes [4]. Figure 4 shows the collaborative BlackHole Attack, where the two malicious nodes are C and D. Node A is the source node and node G is the destination node.

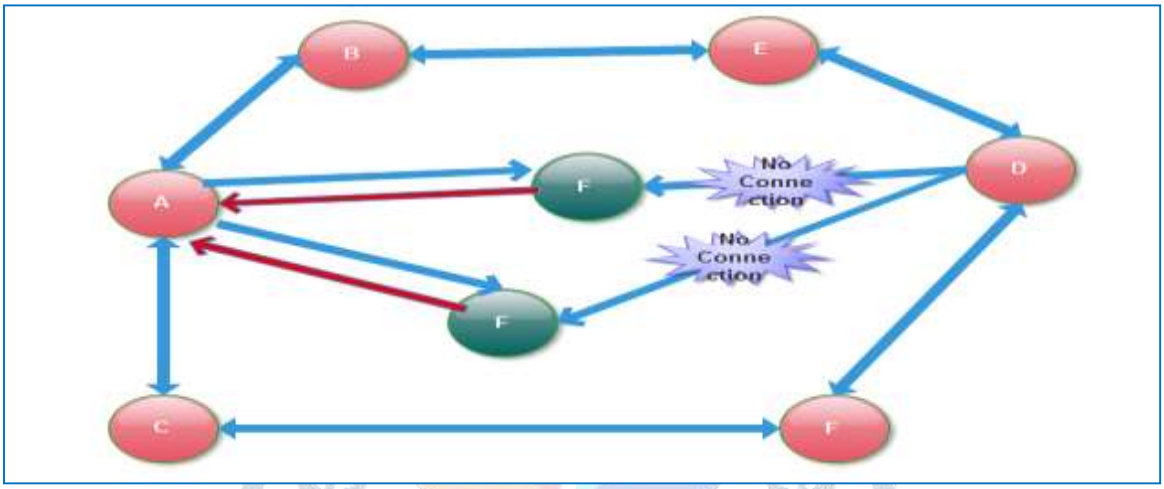

Figure 3: Collaborative Black hole Attack

IV. LITERATURE SURVEY

Before ***"DR scheme and cross-checking scheme" [5, 6]*** Hesiri Weerasinghe planned an algorithmic program to determine the cooperative attack of the black hole. In this case, a slight modification is made to the AODV routing protocol by adding an additional table, that is, a data routing information (DRI) table and a cross check using the additional request - FREQ and the additional response - FREP. The DRI table helps to track whether the node has participated in data transfers with its neighbors. Each entry within the table relative to its neighbor indicates whether the node has sent data through or from that neighbor node. If there are no routes to the destination, the source node can send a route request packet: RREQ to look for a safe path to the destination node, just like in the ODV. Once the intermediate node receives RREQ, it will respond to the request or, once again, transmit it to the network, this will depend on the availability of a new route to the destination. If the destination includes a response, all intermediate nodes update their routing entry for that destination. The source node also sends data on the route because it trusts the destination and updates the DRI table with all the intermediate nodes between the source and, therefore, the destination.

"Detection, prevention and reactive AODV (DPRAODV)" [7] The new package called ALARM is used in the DPRAODV scheme. In this scheme a further check on the threshold value is carried out. The sequence number REP is checked to see if its value is greater than or equal to the threshold value. If the value of the RREP sequence number is greater than the threshold value, the node is called a malicious node and is updated to the blacklist. ALARM is sent to adjacent nodes, each with a black list. So when RREQ comes from a node, the intermediate nodes check if the sending node is in the blacklist, if it is, it will simply reject the packets from that node. This blocks RREP of the malicious node. The advantage of DDPAODV is that it has a higher package delivery ration than the original ODV, but it involves a higher routing overhead and an end-to-end delay. It does not support the cooperative attack of the black hole.

"Time-based threshold detection scheme" [8] Tamilselvan L has proposed a technique that is the improvement of the original AODV routing protocol. The main concept is that, once the first request is found, the collection of requests from other nodes is done via a timer. The Route Collection Response Table (CRRT) is used to collect sequence numbers and time values. By comparing the arrival time of the first request and the threshold value, the value of the network routing request is measured. The result of the simulation shows that a higher percentage of package delivery is achieved with minimal delay and overload. The disadvantage is the end-to-end delay when the malicious node is far from the source node.

"Trusted table method" [9] In this method, each node is given a data structure called a trusted table. This table is responsible for managing the addresses of the trusted nodes. An additional field called as a trust field is attached to the RREP package. This field indicates the reliability of the reply node. Only if RREP is propagated from a reliable node, the source does not send its data through it, otherwise an additional RREP is expected.

The "Routing and neighborhood recovery scheme" [10] in this method detects a black hole attack based on the information in the adjacent set. It consists of two parts: detection and response. Two main steps in the detection procedure are the collection of information from neighboring sets and the search for the black hole attack. In the response procedure, the source node sends a path entry change control packet (MRE) to the destination node to form a precise path by modifying the routing entries of the intermediate nodes from the source to the destination. This scheme is more effective at detecting black hole attacks with less network control overhead. The disadvantage of this scheme is that it becomes useless when the attacker agrees to falsify the packages of false answers.

"Nital mistry et al method" [11] This method proposed a better security of the AODV routing protocol against Blackhole Attack. In this method, the operation of the source node is modified by adding the new Pre_Receive_Reply parameter. Along with this, the Cmg_RREP _Tab table, a Mali variable node and a new MOS _WAIT_TIME timer are also added to the original ODV. In this method, the source node expects MOS _WAIT_TIME after receiving the first RREP and at the same time stores all the RREPs in the _TM _WAIT_TIME table of Cmg_RREP. Now, when analyzing the source node of the stored RREPs, the RREP with a higher target sequence number will be discarded. It is said that a node is a malicious node called a mail node, if the node has sent RREP with a high destination sequence number. It also helps to discard messages from that node in the future. The package delivery ratio increased by 81.812% in the presence of a black hole attack compared to AODV and there is a 13.28% increase in the end-to-end delay.

METHOD	ADVANTAGES	DISADVANTAGES
DR table and cross checking schema	Supports Cooperative Black Hole Attack	Cannot support gray hole attack
Detection, prevention and reactive AODV schema	Packet Delivery Ratio is increased compared to original AODV	Increased routing overhead and end to end delay
Time based threshold detection schema	Higher Packet Delivery ratio with minimal delay and overhead	Increased end to end delay
Trust table Method	Supports the detection of multiple black hole attack	Increased end to end delay
Neighborhood based and routing recovery schema	15% of increased packet throughput	It becomes useless when the attacker agrees to forge the false reply packets
Nital Mistery et al "S-Method"	Supports Black Hole Attack	incresed delay

Figure 4: Comparison of Different Methods

V. CONCLUSION & FUTURE WORK

A Black Hole attack is one of the most important security problems in MANET. During this, a malicious node turns off as a destination node by sending a fake RREP to the source node, collecting all the packets themselves and dropping them. In the AODV routing protocol, the major security threat that degrades performance is the attack of the black hole. Its identification is the main reason for concern. There are several disadvantages of the routing protocols in MANET, so the researchers have carried out numerous techniques to propose different types of detection and prevention mechanisms for the attack of the black hole.

This article presents a survey of several existing techniques for detecting black hole attacks with their defects. These methods have benefits such as increased packet distribution or compatibility with multiple black hole attacks at the same time. All these methodologies have some or the opposite disadvantages, whether it is a higher overload, a greater loss of packets, is not compatible with the black hole cooperative attack or a greater end-to-end delay. Based primarily on previous performance comparisons, it can be concluded that the Black Hole attack has a negative impact on the network. Therefore, there is a desire for detection and perfect elimination of the black hole mechanism based on the organization of cluster networks. This is compatible with the cooperative attack of black holes and, moreover, offers a means for the server node to overcome the error. Therefore, providing security for the black hole attack and effective detection and prevention are the future needs of ad hoc networks.

REFERENCES

[1] Irshad Ullah and Shoaib Ur Rehman, “Analysis of Black Hole Attack on Mobile Ad Hoc Networks using Different Manet Routing Protocols” June 2010.
[2] Sevil Sen, John A. Clark, Juan E.Tapiador, “Security Threats in Mobile Ad Hoc Networks”.

[3] Tarunpreet Bhatia, A.K.Verma, "Security Issues in MANET: A Survey on Attacks and Defense Mechanism", International Journal of Advanced Research in Computer Science and Software Engineering, vol.3, issue 6, pp.1382-1394, 2013.

[4] Kriti Gupta, Maansi Gujral and Nidhi, "Secure Detection Technique Against Blackhole Attack For Zone Routing Protocol in MANETS", International Journal of Application or Innovation in Engineering & Management (IJAIEM), Volume 2, Issue 6, June 2013.
[5] Hesiri Weerasinghe and Huirong Fu, Preventing Cooperative Black Hole Attacks in Mobile Ad Hoc Networks: Simulation Implementation and Evaluation, Intenation Journal of Software Engineering and its Application, Vol.2, Issue 3, July 2008.
[6] Ramaswamy S, Fu H, Sreekantaradhya M, Dixon J, Nygard K, Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks, Paper presented at the International Conference on Wireless Networks, Las Vegas, Nevada, USA, 23-26 June 2003.
[7] Raj PN, Swadas PB, DPRAODV: A Dynamic Learning System against Blackhole Attack in AODV based MANETs, International Journal of Computer Science Issue, Vol. 2, pp 54-59, 2009.
[8] Tamilselvan L, Sankaranarayanan V, Prevention of Blackhole Attack in MANET, 2nd International Conference on Wireless Broadband and Ultra Wideband Communications, Sydney, Australia, 27-30 August 2007.
[9] Yaser khamayseh, Abdulraheem Bader, Wail Mardini, Muneer BaniYasein, in "A New Protocol for Detecting Black Hole Nodes in Adhoc Network, Internalional Journal of COllununication Networks and Infonnation Se curity (IJCNlS), Vol. 3, No. I, April 2011
[10] Sun B, Guan Y, Chen J, Pooch UW , Detecting Black-hole Attack in Mobile Ad Hoc Networks, 5th European Personal Mobile Communications Conference, Glasgow, United Kingdom, 22-25 April 2003.
[11] Mistry N, Jinwala DC, IAENG, Zaveri M, Improving AODV Protocol Against Blackhole Attacks, International MultiConference of Engineers and Computer Scientists IMECS Hong Kong, Vol. 2, pp 1-6, 17-19 March, 2010.
[12] Sagar R Deshmukh, P N Chatur, Nikhil B Bhople, "AODV-Based Secure Routing Against Blackhole Attack in MANET" Published in: IEEE International Conference On Recent Trends In Electronics Information Communication Technology, May 20-21, 2016, India.
[13] NidhiChoudhary, Dr.LokeshTharani, "Preventing Black Hole Attack in AODV using Timer-Based Detection Mechanism" Published in: Signal Processing And Communication Engineering Systems (SPACES), 2015 International Conference on Date of Conference: 2-3 Jan. 2015.