International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 4 Issue 05, May-2015

Review for Detecting Black Holes Attacks in MANET

Comparision and a Survey

Rashika Indoria
Department of Computer Science & Engineering
ITM University
Gwalior, India

Deepak Motwani
Department of Computer Science & Engineering
ITM University
Gwalior, India

***Abstract*— Mobile Ad hoc Network (MANET) is a collection of dynamic mobile nodes which made a temporary infrastructure less network. These networks are completely distributed and also can work at any place without any need of infrastructure. This advantage makes these networks highly robust. MANET has several number of applications mainly are Sensor Networks (SN), medical, military and rescue operations. In Manet Routing consider important component and AODV Ad-hoc On-demand Distance Vector is one of the most accurate routing protocol for detection of black holes attack whether for single black hole attack or cooperative black hole attack. In this paper, we have done a survey and comparisons of the different solutions given by different authors for black hole attacks on AODV protocol and the drawbacks.**

***Keywords*— Ad hoc Network, Black Hole Attack, MANET, AODV.**

I. INTRODUCTION

In networking, an adhoc network means to a network connection accepted for a single session and does not require a router or a wireless base station. A wireless ad hoc network is a connection that is composed of individual devices communicating with each other directly. MANET is a part of wireless ad hoc network that can change its locations and configure itself because this networks are mobile therefore they use wireless connections to connect themselves to various networks. Mobile ad hoc network is a collection of independent mobile nodes that can communicate to each other with the help of radio waves. The mobile ad hoc network has insecure nature because of the freedom for the mobile nodes to join or leave or move inside the network, some of the nodes may be compromised by the enemy and thus perform some malicious behaviors that are hard to detect. MANET is vulnerable to various kinds of attacks. Black hole attack is one of many possible attacks in MANET. Black hole attack can occur when the malicious node on the path directly attacks the data traffic and intentionally leave or delay or change all the data traffic transferring through it. This attack can be easily lessen by setting the promiscuous mode of each node and to see if the next node on the path forward the data traffic as expected. As a result, if we compared it with the wired network then the mobile ad hoc network will need more security scheme to ensure the security of it.

II. SECURITY CHALLENGES IN MANET:

Vulnerability or security is a weakness in any security system. A particular system may be unprotected to unauthorized data manipulation because the system does not verify a user's identity before allowing data access. MANETs are not much more secure to attack than wired network. This is because of the following reasons:

- *Unavailability of central coordinator:* MANET doesn't have a centralized coordinator server. The absence of this management makes the detection of attacks difficult because it is not east to monitor the traffic in a highly dynamic and large scale adhoc network.
- *Absence of predefined boundary:* In mobile ad- hoc networks we cannot exactly define a physical boundary of the network. The nodes work in a free atmosphere in which they have permission to enter or leave the network. As soon as a challenger comes in the radio range of a node it will be able to communicate with that node
- *Dynamic topologies and membership:* A network topology of adhoc network is very active as flexibility of nodes or membership of nodes is very erratic and rapid. This significance the need for secure solutions to be dynamic.
- *Vulnerable wireless link:* Passive or Active link attacks like eavesdropping, spoofing, denial of service, masquerading, impersonation are possible.
- *Cooperativeness in network:* Routing algorithm for MANETs usually assumes that nodes are cooperative and non-malicious. As a result a malicious attacker can easily become an important routing agent and disrupt network operation..

III. Different Security Attacks

There are various kinds of attack in the mobile adhoc network all of which can be classified as the following two type of classification:

Classification I: Passive attack targets the confidentiality attribute of the system. Passive attack is very tough to identify because the performance of the network is not overblown by this type of attack. These are generally used to gather the information about the network or know the communication pattern between the parties. This attack is easy to launch and it may lead to active attack. In Active Attack the intruders can change the packet, insert the packet, drops the packet or it can use the various features of the network to launch the attack. Active Attacks are very dangerous.

Classification II: External attacks: In this attack the attacker aims to cause congestion, propagate fake routing information or disturb nodes from providing services. Internal attacks: It is an attack in which the opponent wants to gain the normal access to the network and participates the network activities by some harmful impression to get the entrance to the network either as a new node or by directly make concession a current node and using it as a basis to conduct its harmful behaviors.

Examples of Security attacks are:

A. Denial of Service (DOS):

Dos Attack attempt to block authorized user from the service offered by the network. The attacker blocks the user from accessing the network resource or congests the network with the excess of vague data packets and prevents the user from accessing the network resources.

B. Black Hole Attack:

A Black-hole is a harmful node that falsely replies for route requests without having an active route to the destination and exploits the Routing Protocol to advertise itself as having a shortest route to destination. By broadcast the shortest path, head station starts sending data through the black hole node and it becomes the active element in the path.

C. Worm Hole Attack:

In this wormhole Attack, an attacker records packets at one location in the network and tunnels them to another location. This tunnel between two colluding attackers is called as a wormhole. Routing can be distorted when routing control messages are tunneled. When this attack is used in opposition for an on-demand routing protocol the attack could prevent the locating of any routes other than through the wormhole.

D. Byzantine Attack:

An undermine intermediate node works alone, or a set of compromised intermediate nodes works in collusion and carry out attacks. These attacker nodes creates routing loops and readdress the packets through non-optimal paths or selectively drops packets, which results in confusion or fortification of the routing services.

E. Sleep Deprivation:

It is also called as resource consumption attack. An attacker or a compromise node can attempt to eat battery life by requesting uncontrolled route discovery for packets or by forwarding unnecessary packets to the victim node.

F. Eavesdropping:

The main aim of eavesdropping is to obtain some confidential information that should be kept secret during the communication. This confidential information may be contain the location, public key, private key or even passwords of the nodes..

G. Flooding Attack:

Flooding Attack can be launched by flooding the network with faker REQs or data packets leading to the congestion of the network and reduces the probability of data transmission of the genuine nodes.

H. Sybil Attack:

In this attack, the attacker node takes the identity of a non existing node and broadcasts multiple non existing identities. A single attacking node usually acts as multiple nodes and take the identity of legitimate node as well. The multiple nodes identities which created by the attacking node are known as Sybil nodes and it can disturb the large part of the network.

IV. EXISTING TECHNIQUES FOR DETECTING BLACK HOLES ATTACK

A number of protocols as a solution were proposed to solve the black hole attack problem. It requires a source node to initiates a checking procedure to determine the reliability of any intermediate node claiming that it has a fresh enough route to the destination.

Romina Sharma ,Rajesh Shrivastava[1] proposed the modified working of AODV protocol by adding RREP message and two other control message including further route request(FRREQ) and further route reply(FRREP).This Proposed solution is for single black hole node. Another part is reduction in packet delivery and throughput but the negative point of this proposed work is that it cannot prevent co-operative black hole attack and second thing the routing overhead also increased because of two extra control message.

Iman Zangeneh, Sehighed Navaezadeh ,Abolfazl Jafare [2] explained about the Adhoc network, nodes, how connection is establish between nodes, and how nodes exchange data than he explained about the AODV routing protocol which he used in his proposed work and then about the black hole attack- that is single black hole and cooperative black hole. In this paper, Author proposed a method which is called Fidelity level which is changed by the source node and also include the timer which makes an advantage of sending the packet to neighbors and wait to collect RREP.This packets are collected until the end of the timer time and then stores in the table called table of response and author also used and equation-

RF=Sequence no.*Nodes Fidelity level

By using this method waiting time is increased and end to end delay and routing over head is increased.

Roopal Lakhwani, Sakshi Suhane, Anand Motwani[3] proposed an agent based aodv protocol which include both detecting and removing of black holes attacks. This paper describes the routing security issue of MANET and Black holes attacks. Author proposed a feasible solution for this in this protocol. In the Protocol "An Agent based AODV" is designed to achieve the objective. The Modification in this algorithm is adding Send Reply()function and RerReply()function which helps to detect the malicious nodes and stop them to participate in the network. This paper shows significant improvement in packet Delivery ratio of Aodv in presence of black hole attack.

Jaspinder kaur, Birinder Singh[4] proposed modification in traditional Aodv protocol to prevent black hole attack. The basic idea for this proposed work is to use of fake message that is using fake route request packets. The fake route request packets contain the IP Address of the node which doesn't exist in the network. As a result the malicious node will reply back this later is detected as the harmful node. The source node get various available path are there, and the source node never select that path in which the node exist with the help of this technique we can easily detect the black hole attack in the network.

Muneer bani yasseins, yaser khamayesh, bahia nawafleh[5] This paper proposes an enhancement to adov routing protocol by engaging successful policies to detect and avoid black hole node. The proposed AODV Protocol attains a remarkable upgrade above both MI-AODV and original AODV protocol in terms of packet delivery ratio, dropped packet ratio, and overhead. In this paper, author proposed to insert a new field in the RREP Message to store the address of the last node that has a path to the destination also black list table contains a list of node with failed RREP Message that exceeded a certain threshold. An Acknowledgment message also added in this proposed work which contains the packet delivery message with 1 and 0.

Neelam khemariya, Ajay khunteta[6] author proposed an efficient approach for the detection and removal of the black hole attack in the manet describe. The proposed algorithm is implemented on aodv routing protocol. This algorithm can detects both the single black hole attack and the cooperative black hole attack. The beauty of the algorithm describe in this paper it is not only detect the black hole nodes in the case when the node is not non-functioning but it can also identify the black hole point in case when the point is not functioning. These two implementation made the approach very secure and efficient.

Komal,Sonam Dhawan[7] Author proposed the work is related with the aodv protocol. We can detect multiple black holes by this protocol if it immediate replies to the RREQ.There will be multiple paths but the proposal chooses only one path. In this proposal protocol, author proposed different message format and message type. The proposed algorithm which author used to detect black hole attack in AOMDV that is adhoc on demand multipath distance vector routing protocol.

Manita, Vinay kumar nassa, Mr. Kapil chawel[8] author proposed the modified Aodv protocol to handle the black hole attack and grey hole attack. This paper modifies the AODV Routing protocol by using ant Colony Optimization. This modified Aodv detect the black hole and grey hole attack and also recover from these attack. The packet delivery ratio is increased and this delay gets reduced and the throughput is also get increased.

Hafessa m habeeb,Selin m[9] The current proposed method in this paper deals with a secure routing protocol to reduce the broadcast problem and the routing overhead in the adhoc network. It can detect the black holes in the network along with implementation of route discovery and black hole detection is also discussed. Author proposed a solution to detecting the malicious node in neighbor coverage probabilistic protocol (NCPR) suffering from black hole attack. The new thing which author added is DSR routing in the adhoc network.

Manisha Sao, Sushil Kashyap ,Dr.Vishnu kumar Mishra[10] The main motive of this research work is to improve the main advantage of this protocol that is routes are established on demand and destination sequence number are used to search out the newest route to the destination. In this paper author proposed a method which is called route discovery method. In this method basically the sender node broadcast the method to its neighbor so that the receiver node respond for this method but the sender node is not directly connected with the receiver node so that the neighbor of this node connects the sender to the receiver and then the RERP message forwarded by the receiver and all the sending of nodes are basically done by the sequence number. The AODV plays an important role in it. The RERP (Route error message) allows AODV to adjust routes when nodes move around.

Ashish Sharma , Dinesh Bhuriya ,Upendra Singh , Sushma Singh[11] The Author Proposed a different algorithm that is TAODV. The new Trust based AODV algorithm is used in this paper. The basic method which author proposed is the algorithm uses sequence number. This AODV algorithm includes three message- Route Request that is (RREQ), Route reply that is (RREP) and route error that is (RERR). This algorithm maintains routing table and keep on updating the table content field while recover a routing message. In this paper, author proposed three factor of TAODV algorithm that is unreliable node, reliable node and most reliable node. During these three phases, the route discovery will be there.

V. COMPARISION TABLE

In this table,we are comparing all the existing techniques for the detection of black hole attack and we also mentioned the assumption for this proposed work and the result which we got.

TABLE I. COMPARISON OF VARIOUS BLACK HOLE ATTACK DETECTION METHOD

Proposal Name	Approach	Assumption	Philosophy
Modified AODV protocol to prevent black hole attack.	AODV	Multiple Black Hole	Single Black Hole node
New method for detection and prevention single black holes attack	AODV	Single Black Hole	Single Black Hole
Agent based Aodv protocol for detection and removal of Black hole attack	Agent based AODV	Multiple and Cooperative black hole	Single Black Hole
Detection and isolate black Hole Attack	AODV	Multiple and Cooperative black hole	Single Black Hole attack
Detect and avoid black hole attack	AODV, MIAODV	Multiple and Cooperative black hole	Single Black Hole attack
Rebroadcast routing protocol for black hole	NCPR DSR	Single Black Hole	Single Black Hole
Efficient algorithm for detection of black hole attack	AODV	Single and cooperative black hole nodes	Single and cooperative black hole nodes
Improved AODV protocol for black hole detection	AODV	Single and cooperative black hole nodes	Single and cooperative black hole nodes
AODV protocol against Black Hole and Grey Hole Attack	AODV	Black hole and grey hole node	Black hole and grey hole node attack
Prevention of black hole attack using Trust based computing	TAODV	Cooperative black hole nodes	Single Black Hole Attack

[a.] Sample of a Table footnote. *(Table footnote)*

VI. CONCLUSION

The various mentioned authors have given various proposals for prevention, detection and removal of black holes attack in MANET but these proposals have some limitation with the given solutions. Some approaches leads to black hole node detection and prevention but also no one is reliable procedure since all the mobile nodes in the network cooperate together to analyze and detect and remove possible not a single but multiple black hole nodes. Future work includes developing simulation to analyze the performance of the proposed solution and can also give a better and different proposal and compare their performance.

VII ACKNOWLEDGMENT

I express my deep sense of gratitude to Associate Professor Mr. Deepak Motwani in the Department of Computer Science & Engineering, ITM University Gwalior. Whose kindness valuable guidance and timely help encouraged me to complete this paper.

VIII REFERENCES

[1] Ronima Sharma, Rajesh Shrivastava, "Modified AODV Protocol to Prevent Black Hole Attack in Mobile Ad-hoc Network," in IJCSNS International Journal of Computer Science and Network Security, VOL.14 No.3, March 2014.

[2] Iman Zangeneh, Sedigheh Navaezadeh, Abolfazl Jafari, "Presenting a New Method for Detection and Prevention of Single Black Holes Attack in AODV Protocol in Wireless Ad Hoc Network", in International Journal of Computer Applications Technology and Research Volume 2– Issue 6, 686 - 689, 2013.

[3] Roopal Lakhwani, Sakshi Suhane,Anand Motwani, "Agent based AODV Protocol to Detect and Remove Black Hole Attacks," in International Journal of Computer Applications (0975 – 8887) Volume 59– No.8, December 2012.

[4] Jaspinder Kaur,Birinder Singh, "Detect and Isolate Black Hole Attack in MANET using AODV Protocol," in International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 3, Issue 2, February 2014.

[5] Muneer Bani Yassein, Yaser Khamayseh, Bahaa Nawafleh, "Improved AODV Protocol to Detect and Avoid Black Hole Nodes in MANETs,"in The Sixth International Conference on Future Computational Technologies and Applications.

[6] Neelam Khemariya, Ajay Khuntetha,"An Efficient Algorithm for Detection of Blackhole Attack in AODV based MANETs"in International Journal of Computer Applications (0975 – 8887) Volume 66– No.18, March 2013.

[7] Komal,Sonam Dhawan," An Improved Performance of MANET using AODV Protocol for Black Hole Detection" in International Journal of Research in Computer and Communication Technology, Vol 3, Issue 5, May- 2014.

[8] Manita, Dr. Vinay Kumar Nassa, Mr.Kapil Chawala "Improving AODV Protocol by Nature Inspired Technique Against Blackhole and Greyhole Attacks in MANETs," in International Journal of Advanced Research in Computer Science and Software Engineering Volume 4, Issue 8, August 2014.

[9] Hafessa M Habeed,Selin.M "A Secure Probabilistic Rebroadcast Routing Protocolbased on Neighbor Coverage in Mobile Adhoc Networks" in International Journal of Advanced Trends in Computer Science and Engineering, Vol.3 September 2014.

[10] Manisha Sao,Sushil.Ku.Kashyap,Dr.Vishnu Kumar Mishra"Preventing Black Hole Attack in Manet Using On-Demand Distance Vector" in International Journal for Research in Applied Science and Engineering Technology Vol.2 Issue V,May 2014.

[11] Ashish Sharma , Dinesh Bhuriya ,Upendra Singh , Sushma Singh" Prevention of Black Hole Attack in AODV Routing Algorithm of MANET Using Trust Based Computing" in International Journal of Computer Science and Information Technologies, Vol. 5 (4) , 2014.

[12] Mohamed Amnai, Youssef Fakhri, Jaafar Abouchabaka, "Evaluation of Impact of Traffic VBR and Mobility on the Performance of AODV Routing Protocols in Mobile Ad hoc Networks", IEEE, 2010.

[13] Mariannne. A. Azer, "Wormhole Attacks Mitigation in Ad Hoc Networks", IEEE 2011, pp 561-568.

[14] [20] Mohamed Amnai, Youssef Fakhri, Jaafar Abouchabaka, "Evaluation of Impact of Traffic VBR and Mobility on the Performance of AODV Routing Protocols in Mobile Ad hoc Networks", IEEE, 2010.

[15] Jayanta Biswas, Mukti Baraiand, and S.K.Nandy "Efficient Hybrid Multicast Routing Protocol for Ad-Hoc Wireless Networks" IEEE.

[16] Subash Chandra Mandhata, and Dr.Surya Narayan Patro", "A counter measure to Black hole attack on AODV- based Mobile Ad-Hoc Networks", IJCCT, 2011.