ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 10, October 2013

Detection & Prevention Techniques to Black & Gray Hole Attacks In MANET: A Survey

Nitesh A. Funde[1], P. R. Pardhi[2]

M Tech Scholar, Department of Computer Science, RCOEM, Nagpur, India [1]

Professor, Department of Computer Science, RCOEM, Nagpur, India [2]

Abstract: Mobile ad hoc network (MANET) is a self-configuring network of mobile nodes formed anytime and anywhere without the help of a fixed infrastructure or centralized management. It has many potential applications in disaster relief operations, military network, and commercial environments. Due to open,dynamic,infrastructure-less nature, the ad hoc networks are vulnerable to various attacks.AODV is an important on-demand distance vector routing protocol for mobile ad hoc networks. It is more vulnerable to black & gray hole attack. In MANET, black hole is an attack in which a node shows malicious behaviour by claiming false RREP message to the source node and correspondingly malicious node drops all the receiving packets. In this paper, we have reviewed different techniques to prevent black & gray hole attacks in MANET.

Keywords: AODV, Black Hole, MANET, Gray Hole

I. INTRODUCTION

In an ad-hoc network, mobile nodes communicate with each other using multihop wireless links .The infrastructure is not fixed that is changing with dynamic topology. Each node in the network acts as a router, forwarding data packets to other nodes [1].

MANET have many potential applications, in military rescue operations and commercial environments. Mobile ad hoc networks are having several security issues due to their inherent nature, like open medium, dynamic topology, lack of centralized control, limited battery power and limited bandwidth[2].Hence, there exist several attacks that can be easily launched on an ad hoc network. Since, wireless networks came into existence, routing in mobile ad hoc networks has been a challenging task. The major reason for this is the constant changes in network topology due to the mobility of nodes.

The routing protocols in MANET are mainly categorized into proactive routing protocols, reactive routing protocols and hybrid routing protocol [3] In proactive routing protocols, the routing information of nodes is exchanged, sporadically, such as DSDV. In reactive routing protocols, nodes exchange routing information when it is needed such as AODV [4].Some ad-hoc routing protocols are a combination of the above two categories called as hybrid routing protocols.These routing protocols plays an important role in determining efficient route between a pair of nodes so that messages can be delivered in a timely manner. In the following, Section 2 provides description of AODV protocol and factors that leads to attacks on network layer, section 3 describes the way black hole attack *is* performed on AODV and Section 4 describes gray hole attack .Section5 deals with several techniques to prevent black hole attack, section 6 describes the techniques to detect gray hole attack and last section presents conclusion and future work of paper.

Fig. 1. MANET

II. AODV ROUTING PROTOCOL

AODV is an ad-hoc on demand distance vector routing protocol that establishes route to the destination when it is desired by the source node. It maintains this routes as and when needed by the source node. It offers quick adaptation to dynamic link conditions, low processing, memory overhead, low network utilization, and determines unicast routes to destinations within the ad hoc network [1].

One of the distinguishing feature of AODV protocol is its use of destination sequence number associated with every route. Destination sequence number is created by the

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 10, October 2013

destination to include route information about it send to the requesting node. In order to communicate among the mobile nodes, [1] Route Requests (RREQs), Route Replies (RREPs), and Route Errors (RERRs) are the message types defined by AODV. When a source node wants to connect to a destination node, first it checks in the existing route table, as to whether a fresh route to that destination is available or not.

Fresh enough route means a valid route entry whose sequence number is greater than it in the RREQ. Larger the sequence number, fresher is the route. If a fresh enough route is available, it uses the same. Otherwise the node initiates a Route Discovery by broadcasting a RREQ control message to all of its neighbors. This RREQ message will further be forwarded by the intermediate nodes to their neighbors having a fresh route to the destination.

The RREQ message will eventually reach the destination node, which will react with a route reply message (RREP). The RREP is sent as a unicast to the source node along the reverse route established during the RREQ broadcast. Similarly, the RREP message allows intermediate nodes to learn a forward route to the destination node. Therefore, at the end of the route discovery process, packets can be delivered from the source node to the destination node and vice versa. A route error message (RERR) allows nodes to notify errors due to link breakage, such as when a previous neighbor moves to a new position and is no longer reachable. Each mobile node would periodically send Hello messages (HELLO), thus, each node knows which nodes are its neighboring nodes.

AODV as a reactive routing protocol, does not give nodes a complete view of network topology. That is, each node only knows its neighbors, and for the non-neighbors, it only knows the next hop to reach them and the distance in hops. However, the security of AODV is compromised by the Black Hole nodes, as it accepts the received RREP having fresher route.

The standard AODV routing protocol can not fight the threat of Black Hole attacks, because during the phase of route discovery, malicious nodes may counterfeit a sequence number and hop count in the routing message; thereby, acquiring the route [3] , eavesdropping and dropping all the data packets as they pass or forward some selective packets to the destination.

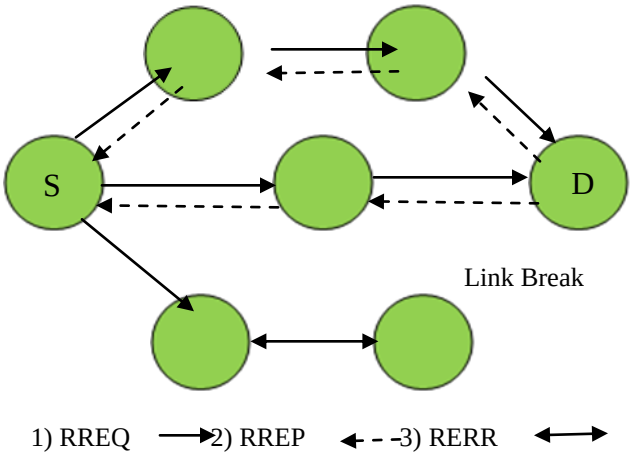


Fig. 2. Working Of AODV Protocol

III. BLACK HOLE ATTACK

In the figure 3, consider a malicious node M. When node 1 broadcasts a RREQ packet; nodes 2,4 and M receive it. Node M, being a malicious node, does not check up with its routing table for the requested route to node 5. Hence, it immediately sends back a false RREP packet, claiming a shortest route to the destination. Node 1 Receives the RREP from M ahead of the RREP from 2 and 4.Node 1 assumes that the route through M is the shortest route and sends data packets to the destination through it. When the node 1 sends data to M, it absorbs all the data and drops this data. As this data can not reach to the destination It is called as a Black hole attack.

Therefore, source and destination nodes are unable to communicate with each other [2]. The malicious node always sends RREP as soon as it receives RREQ without performing standard AODV operations, while keeping the Destination Sequence number very high. Since AODV considers RREP having higher value of destination sequence number to be fresh, the RREP sent by the malicious node is treated fresh. Thus, malicious nodes succeed in injecting Black Hole attack.

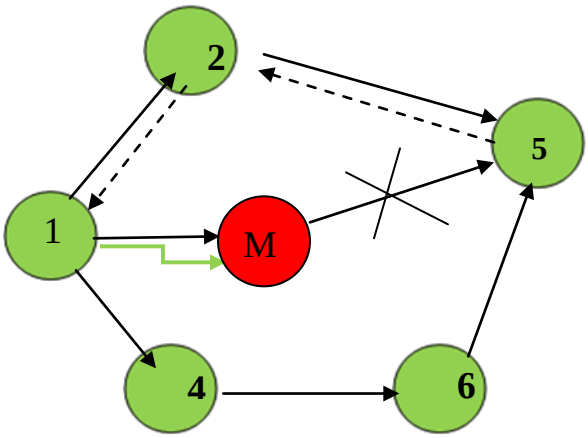
IV. GRAY HOLE ATTACK

Gray hole attack [3] is a special variation of black hole attack, where nodes switch their states from black hole to honest intermittently and vice versa. It is difficult to detect gray hole attack because nodes can drop packets partially and behaves like a normal honest node. Figure2 shows the black hole attack. But if Node M forward data completely or partially to the destination. It may send some selective packets and drops an important data.This type of attack is called as gray hole attack.

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 10, October 2013

Therefore detection is difficult because the node's nature is not stable, it can't predicted that when node will be malicious and when it will turn to normal node. Node 1 selects gray hole M even node 2 has valid and shortest path to destination.



M- Malicious node Data:

Fig.3 Black Hole Attack

V. RELATED WORKS IN BLACK HOLE ATTACK

A. Next Hop Information Based Scheme

Deng et.al [4] have discussed discuss a protocol that requires the intermediate nodes to send RREP message along with the next hop information. When the source node get this information, it sends a RREQ to the next hop to verify that the target node (i.e. the node that just sent back the RREP packet) indeed has a route to the intermediate node and to the destination. When the next hop receives a Further Request, it sends a FurtherReply which includes the check result to the source node. Based on information in FurtherReply, the source node judges the validity of the route.

In this protocol, the RREP control packet is modified to contain the information about next hop. After receiving RREP, the source node will again send RREQ to the node specified as next hop in the received RREP.However, this increases the routing overhead and end-to-end delay. In addition, the intermediate node needs to send RREP message twice for a single route request.

B. *DPRAODV : Detection Prevention Reactive Scheme*

Raj PN et.al [9] discuss a protocol viz. DPRAODV (Dynamic, Prevention and Reactive AODV) to counter the Black hole attacks. Unlike normal AODV, DPRAODV checks to find whether the RREP_Seq_No is higher than the threshold value. In this protocol, the threshold value is dynamically updated at every time interval. If the value of RREP_Seq_No is found to be higher than the threshold value, the node is suspected to be malicious and is added to a list of blacklisted nodes. It also sends an ALARM packet to its neighbors with information about the blacklisted node. Thus, the neighbor nodes know that RREP packets from the malicious node are to be discarded. That is, if any node receives the RREP packet, it looks over the list to check the source of the received message. If the reply is from the suspected node, the same is ignored.

In the simulation results, the packet delivery ratio is improved by 80-85% than AODV when under black hole attack, and 60% when traffic load increases. The advantage of DPRAODV is that it achieves an obviously higher packet delivery ratio than the original AODV. Thus, the protocol though successful, suffers from the overhead of updating threshold value at every time interval and generation of the ALARM packets. The routing overhead, as a result is higher.

C) IDAD Mechanism

In this, [10] author proposed a solution based on Intrusion Detection using Anomaly Detection (IDAD). It prevents both attacks by single and multiple black hole nodes. IDAD assumes every activity of a user can be monitored and anomaly activities of an intruder can be identified from normal activities. To find a black hole node IDAD needs to be provided with a pre-collected set of anomaly activities, called audit data. Once audit data collected and it is given to the IDAD system, which is able to compare every activity with audit data. If any activity of a node is out of the activity listed in the audit data, the IDAD system isolates the particular node from the network. The reduction of the number of routing packets in turn minimizes network overhead and facilitates a faster communication. But the drawback is that if neighbor node give false information then this solution gives more delay in the net-work.

D. Nital Mistry's Method

The author proposed a solution for analyzing and improving the security of AODV routing protocol against black hole attack. The approach basically modifies the working of source node only, using additional function pre_receivereply [6]. A table cmg_rrep_tab, a variable mali_node and a new timer mos_wait_time are data strucures added to the default AODV. In the proposed solution, after receiving the first RREP the source node waits for mos_wait_time and meanwhile it stores all the rreps in the cmg_rrep_tab table until mos_wait_time.In this technique the value of mos_wait_time is considered to be half the value of rrep_wait_time. Now, the source node will analyze the stored RREP and will discard the RREP which have high destination sequence number. The node which has

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 10, October 2013

sent these RREP with high destination sequence number are considered to be malicious node. This technique also declare the identity of suspected malicious nodes as mail_node , so that in future it can discard messages coming from that node and the routing table is not maintained for that node The packet delivery ratio is increased by 81.812% in presence of black hole attack compared to AODV and there is 13.28% rise in end-to end delay. The disadvantage of this method it fails to detect collaborative black hole attack.

E. Sequence Number Based Scheme

An algorithm presented in [5] to detect the black hole attack in a MANET based on the preprocessor called Pre_Process_RREP and it is simple and does not change workings of either intermediate or destination node. It does not even modify the working of normal AODV . The Process continues to accept RREP packets and calls a process called Compare_Pkts (packet p1, packet p2) which actually compares the destination sequence number of two packets and selects the packet with higher destination sequence number if the difference between two numbers is not significantly high. Packet containing exceptionally high destination sequence number is suspected to be a malicious node and an ALERT message containing the node identification is generated which is broadcasted to neighbor nodes so that it can be isolated from the network and can maintain a list of such malicious nodes. This solution has more network delay and cannot detect cooperative black hole Nodes.

VI. RELATED WORKS IN GRAY HOLE ATTACK

A. Path Based Mechanism

Jiwen CAI et.al proposed a path-based method in network layer, to overhear the next hop's action [7]. Here , a node does not watch every node in the neighbor, but only observes the next hop in current route path. every node should keep a FwdPktBuffer, which is a packet digest buffer. When a packet is forwarded out, its digest is added into the FwdPktBuffer and the detecting node overhears. Once the action that the next hop forwards the packet is overheard, the digest will be released from the FwdPktBuffer.In a fixed period of time, the detecting node should calculate the overhear rate of its next hop and compare it with a threshold. Author define overhear rate in the Nth period of time as (total overheard packet no/total forward packet no).In this scheme, each node only depends on itself to detect a gray hole. The algorithm does not send out extra control packets so that Routing Packet Overhead is not more. This method involves too much calculation.

B. Optimal Path & Hash Based Scheme

The Author proposed a solution is the avoidance of black and gray hole attacks by discarding the first and selecting the second shortest path for data packets transmission [8] .First ,it prevents gray hole attacks by selecting the safe and secure route for data packets transmission. Second, it provides more security for data integrity and further detection of malicious node on the safe route. When source node receives RREP messages from different nodes connected with destination, it just discards the first RREP message coming from any intermediate node connected with destination for the avoidance of black /gray hole. In this solution, source selects second shortest route for transmission of data packets to destination rather than selecting the first optimal route. This solution avoids black hole / gray hole attacks in such a way that by using the second shortest path for data packets transmission, it would be hard for black hole or gray hole node to monitor the entire network to know where to place itself in a network and mislead the source node that it has the second shortest route to the destination. This scheme is not implemented yet.

VII. CONCLUSION

In this paper, a survey on detection and prevention techniques of black & gray hole attack in MANET is presented. A Black & Gray Hole attack are serious attacks in MANET. Black hole is an attack where a malicious node do not forward the data packets to the destination and gray hole attack is a special variation of black hole attack which is difficult to detect. Based on the above survey, it can be concluded that Black Hole and gray attacks are severe attacks and can affect the AODV routing protocol in MANET negatively. Hence, there is need for good detection and elimination mechanisms for these attacks. Future work is intended to find presence of these attacks in MANET, if present then we will detect it and confirm it whether it is black hole or gray hole attack and finally eliminate these attacks from the network.

ACKNOWLEDGMENT

I express my sincere gratitude to Dr. M. B. Chandak, Head Department of CSE, for his valuable guidance and advice. Also I would like to thanks to my guide Prof. P .R. Pardhi and the faculty members for their continuous support and encouragement.

REFERENCES

[1] C. Perkins. "(RFC) request for Comments-3561", Category: Experimental, Network, Working Group, July 2003.
[2] Ebrahim Mohamad, Louis Dargin. "Routing Protocols Security." In: Ad Hoc Networks". A Thesis at Oakland University School of Computer Science and Engineering.
[3] Dokurer,Seimih "Simulation of Black hole Attackin wireless ad-hoc Networks" Master's Thesis Atihm University,Septeber 2006

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

[4] Deng H., Li W. and Agrawal, D.P., "Routing security in wireless ad hoc networks," Communications Magazine, IEEE, vol.40, no.10, pp. 70- 75, October 2002

[5] Subash Chandra Mandhata, Dr.Surya Narayan Patro, "A counter measure to Black hole attack on AODV- based Mobile Ad-Hoc Networks" International Journal of Computer & Communication Technology.volume-2, Issue- VI,2011

[6] Nital Mistry, Devesh C Jinwala, Mukesh Zaveri, "Improving AODV Protocol against Blackhole Attacks", proceedings of the International Multi Conference of Engineers and Computer Scientists 2010 Vol II, IMECS 210

[7] 2010 24th IEEE International Conference on Advanced Networking and Applications An Adaptive Approach toDetecti Black and Gray Hole Attacks in Ad Hoc Network Jiwen CAI, Jialin CHEN, Zhiyang WANG, Ning LIU

[8] Preventing Black and Gray Hole Attacks in AODV using Optimal Path Routing and Hash. Hizbullah Khatt ak, Ni-zamuddin, F ahad Khurshid, Noor ul Amin 2013 IEEE

[9] Payal N. Raj1 and Prashant B. Swadas2, "DPRAODV: A Dynamic Learning System against Blackhole Attack in AODV based MANET", IJCSI International Journal of Computer Science Issues, Vol. 2, 2009.

[10] Alem, Y.F.; Zhao Cheng Xuan; , "Preventing black hole attack in mobile ad-hoc networks using Anomaly Detection," Future Computer and Communication (ICFCC), 2010 2nd International Conference on , vol.3, no., pp.V3-672-V3-676, 21-24 May 2010.