Proc. of the Second Intl. Conf. on Advances in Electronics, Electrical and Computer Engineering -- EEC 2013

ISBN: 978-981-07-6935-2

Detection of Black hole attack in Mobile ADHOC Networks

[Shashi Gurung] [Aditya Kumar] [Dr. Krishan Kumar Saluja]

***Abstract*—Mobile ad hoc networks (MANET) are widely used in that places where there is no available infrastructure. It is also called infrastructure less network. MANET is particularly vulnerable to various types of security attacks due to its fundamental characteristics, e.g. the lack of centralized monitoring, dynamic network topology, open medium, autonomous terminal and management. The black hole attack is one of such security issue in MANET. In this attack, a malicious node gives false information of having shortest route to the destination node so as to get all data packets and drops it. In this paper, we propose an algorithm to detect and prevent black hole attack in AODV routing. The proposed method uses conformation acknowledgment request to check whether the destination has received dummy packet or not.**

Keywords—AODV, Black hole attack, MANET routing protocols, Security)

I. Introduction

The tremendous growth of laptops and 802.11/Wi-Fi wireless networking have made MANETs a popular research topic since the mid-1990s. MANET is a collection of infrastructure less nodes which cooperates with each other to form temporary network. It consists of a collection of wireless mobile nodes that have capability to communicate with each other without the use of network infrastructure or any centralized administration. Also security is important to provide protected communication between nodes in a potentially hostile environment. Although security has long been an active research topic in wire line networks, the unique characteristics of MANETs present a new set of challenges to security design. These challenges include shared wireless medium, highly dynamic network topology, open network architecture and stringent resource constraints. Consequently, the existing security solutions for wired networks do not directly apply to the MANET domain**.** Routing protocol in MANET is divided into two main categories, proactive and reactive. In proactive routing protocols, routing information of nodes is exchanged, periodically, such as DSDV. In on-demand routing protocols, route is established and nodes exchange routing information when needed such as AODV [2]. Furthermore, some ad-hoc routing protocols are a combination of above categories.

II. Overview of AODV

The Ad Hoc On-Demand Distance Vector (AODV) routing protocol is an adaptation of the DSDV protocol for dynamic link conditions [1][2].The AODV uses an on-demand approach for finding route i.e. a route is established only when it is required by a source node for sending data packets. It uses destination sequence numbers to identify the most recent path. Every node in an Ad-hoc network maintains a routing table, which contains information about the path to a particular destination. Whenever a node wants to send packet, it first checks its routing table to check whether a route to the destination is already exist. If so, it uses that path to send the packets to the destination. If a path is not available or the previously entered path is inactivated, then the node starts a route discovery process. A RREQ (Route REQuest) packet is broadcasted by the node. Every node that receives the RREQ packet first checks if it is the destination for that packet and if so, it sends back an RREP (Route REPly) packet. If it is not the destination, then it checks with its routing table to determine if it has fresh route to the destination. If not, it sends the RREQ packet by broadcasting it to its neighbors. If its routing table does contain an entry to the destination, then the comparison of the destination sequence number in its routing table with the destination sequence number present in the RREQ packet is done. This Destination Sequence number is the sequence number of the last sent packet from the destination to the source. If the destination sequence number present in the routing table is lesser than or equal to the one contained in the RREP packet, then the node update its routing table. If the number in the routing table is higher than the number in the packet, it denotes that the route is a fresh route and packets can be sent through this route. This intermediate node then sends a RREP packet to the node through which it received the RREQ packet. The RREP packet gets relayed back to the source through the reverse route. The source node then updates its routing table and sends its packet through this route. During the operation, if any node identifies a link failure it sends a RERR (Route ERRor) packet to all other nodes that uses this link for their communication to other nodes. Since AODV has no security mechanisms, malicious nodes can perform many attacks just by not behaving according to the AODV rules. A malicious node M can carry out many attacks against AODV. This paper provides routing security to the AODV routing protocol by eliminating the threat of Black Hole attacks.

III. Black hole Attack

A Black Hole attack [3] is a kind of denial of service attack where a malicious node gives false information of having shortest route to the destination in order to get all the data packets and drop it. In the following Figure 1. , imagine a malicious node M. When node S broadcasts a RREQ packet, other neighbor node receives it. Node M, being a malicious

Proc. of the Second Intl. Conf. on Advances in Electronics, Electrical and Computer Engineering -- EEC 2013

ISBN: 978-981-07-6935-2

node, does not check up with its routing table for the requested route to node D. Hence, it immediately sends back a RREP packet, claiming of having shortest path to the destination. Node S receives the RREP from M immediately and assumes that the route through M is the shortest route and sends packet to the destination through it. When the node S sends data to M, it absorbs all the data and drop the packets thus behaving like a Black hole.

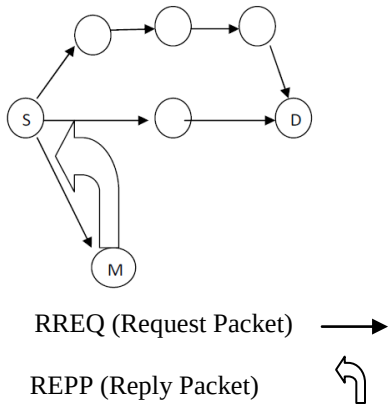


Figure 1. Black hole Attack in AODV

IV. Related Work

H. Deng et al. [3] discussed a protocol that requires the intermediate nodes to send RREP message along with the next hop information. When the source node gets 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 Further Reply which includes the check result to the source node. Based on information in Further Reply, 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.

B. Sun et al. [4] use AODV as their routing protocol and simulation is done in ns2 simulator. The detection scheme used neighborhood-based method to detect the black hole attack and then present a routing recovery protocol to build the true path to the destination. Based on the neighbor set information, a method is designed to deal with the black hole attack, which consists of two parts: detection and response. In detection procedure, two major steps are: Step 1- Collect neighbor set information. Step 2-Determine whether there exists a black hole attack. In Response procedure, Source node sends a modify-Route-Entry (MRE) control packet to the Destination node to form a correct path by modifying the routing entries of the intermediate nodes (IM) from source to destination.

S. Ramaswamy et al. presented an algorithm in [5] which claims to prevent the cooperative black hole attacks in ad-hoc network. In this algorithm each node maintains an additional Data Routing Information (DRI) table. Moreover, in the case when the network in not under the attack, the algorithm takes more time to complete. This algorithm is based on a trust relationship between the nodes, and hence it cannot tackle gray hole attacks

M. Al-Shurman , S-M. Yoo and S. Park [6] proposed two different approaches to solve the black hole attack The first solution the sender node needs to verify the authenticity of the node that initiates the RREP packet by utilizing the redundancy of the network. The idea of this solution is to find more than one route for the destination. The drawback of the solution is the time delay. The second solution is to store the last sent packet sequence number and the last received packet sequence number in the table. It is updated when any packet is arrived or transmitted. When node receives reply from another node it checks the last sent and received sequence number. If there is any mismatch then an ALARM indicates the existence of a black hole node. This method is faster and more reliable and has no overhead..

L. Tamilselvan et al. [7] proposed an approach in which the requesting node waits for the responses including the next hop details, from other neighboring nodes for a predetermined time value. After the timeout value, it first checks in the CRRT (Collect Route Reply Table) table, whether there is any repeated next-hop-node or not. If any repeated next-hop-node is present in the reply paths, it assumes the paths are correct or the chance of malicious paths is limited.

H. Weerasinghe, Fu [8] proposed a solution in which information about the next hop to destination should be included in the RREP packet when any intermediate node replies for RREQ. Then the source node sends a further request (FREQ) to next hop of replied node and asks about the replied node and route to the destination. By using this method we can identify trustworthiness of the replied node only if the next hop is trusted. However, this solution cannot prevent cooperative black hole attack on MANETs.

L. Tamilselvan and Dr. V.Sankaranarayanan [9] also proposed a revised AODV routing protocol, called PCBHA (Prevention of a Co-operative Black Hole Attack), in order to prevent cooperative black holes. First, it provides each legal user with a default fidelity level, and after broadcasting a RREQ, a source node waits to receive returned RREPs from the neighboring nodes, and then selects a neighboring node of a higher fidelity level, which exceeds the threshold value, for passing the data packets. The destination node will return an ACK message after receiving data packets, and the source node may add 1 to the fidelity level of the neighboring node, upon receipt of an ACK response. If no ACK response is received, 1 is subtracted from the fidelity level, which indicates a possible black hole node on this route, and data packets are dropped before reaching the destination node.

M. Medadian et al. [10] have proposed an approach to mitigate the Black hole attack through the judgment process by using honesty of nodes, which, is derived from the opinions of a neighbor nodes of a node in a network. In order to transfer the

Proc. of the Second Intl. Conf. on Advances in Electronics, Electrical and Computer Engineering -- EEC 2013

ISBN: 978-981-07-6935-2

data packets, a node must show its honesty. If a node is the first receiver of a RREP packet, it forwards packets to source and initiates judgment process on about replier. The judgment process was depends on opinion of network's nodes about replier. These neighbors are requested to send their opinion about a node. When a node collects all opinions of neighbors, it decides if the replier is a malicious node based on number rules.

N. Mistry et al. [11] 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. A table Cmg_RREP_Tab, a variable Mali_node and a new timer MOS_WAIT_TIME are also 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 RREPs and will discard the RREP which have high destination sequence number. The node which has sent these RREP with high destination sequence number is considered to be malicious node.

M.Y. Su [12] proposed the mechanism to detect and separate malicious nodes, which selectively perform black hole attacks by deploying IDSs in MANETs (mobile ad hoc networks). All IDS nodes perform an ABM (Anti-Black hole Mechanism), which estimates the suspicious value of a node, according to the amount of abnormal difference between RREQs and RREPs transmitted from the node. With the prerequisite that intermediate nodes are forbidden to reply to RREQs, if an intermediate node, which is not the destination and never broadcasts a RREQ for a specific route, forwards a RREP for the route, then its suspicious value will be increased by 1 in the nearby IDS's SN (suspicious node) table. When the suspicious value of a node exceeds a threshold, a Block message is broadcasted by the detected IDS to all nodes on the network in order to cooperatively isolate the suspicious node.

K. Liu and J. Deng [13] proposed 2ACK scheme to detect and mitigate the effect of such routing misbehavior. The 2ACK technique is based on a simple 2-hop acknowledgment packet that is sent back by the receiver of the next-hop link. Compared with other approaches to combat the problem, such as the overhearing technique, the 2ACK scheme overcomes several problems including ambiguous collisions, receiver collisions, and limited transmission powers. The 2ACK scheme can be used as an add-on technique to routing protocols such as DSR in MANETs hope node for whole transmission. Thus Black hole attacks can greatly be detected and reduced.

TABLE1. DRAWBACKS OF DETECTION METHOD

No.	Methodology proposed by	Attack	Drawbacks
1	H. Deng et al. [3]	Single black hole	1-Cannot prevent cooperative black hole attack. 2-Routing Overhead.
2	B. Sun et al. [4]	Single black hole	Becomes useless when the attacker agrees to forge the fake reply packets
3	S. Ramaswamy et al. [5]	Cooperative black hole	Cannot tackle gray hole attacks
4	M. Al-Shurman et al. [6]	Single black hole	1-Time Delay. 2-Attacker can listen to the channel and update the tables for last sequence number.
5	L. Tamilselvan and Dr.V. Sankaranarayanan [7]	Single black hole	1-Time delay. 2-Finding repeated next hop is an additional overhead.
6	H. Weerasinghe, H. Fu [8]	Cooperative black holes	5-8% more communication overhead of route request.
7	L. Tamilselvan and Dr.V. Sankaranarayanan [9]	Cooperative black holes	Time Delay
8	M. Medadian et al. [10]	Cooperative black holes	Opinion of neighbor's may not always correct
9	N. Mistry et al. [11]	Single black hole	1-Time delay 2-Failed to detect cooperative black hole attack
10	M.Y. Su [12]	Multiple Black holes	Time Delay

V. Proposed Methodology

In this section, we propose a solution to identify black hole node, remove that node from routing table and finally added to the blacklist table. Following is the diagram showing black hole attack.

Proc. of the Second Intl. Conf. on Advances in Electronics, Electrical and Computer Engineering -- EEC 2013

ISBN: 978-981-07-6935-2

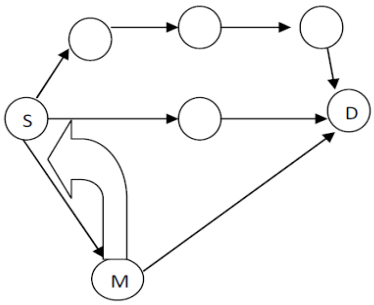


Figure 2. Link between M and D

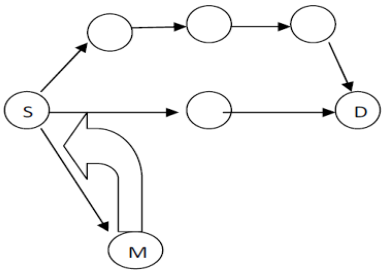


Figure 3. No link between M and D

RREQ (Request Packet)

REPP (Reply Packet)

A. Matrix Representation

TABLE 2. TRUTH TABLE OF MALICIOUS NODE

FIGURE No.	Shortest route to destination	Malicious Node	Packet Drop
4	T	T	T
5	F	T	T

From above representation, it is shown that if there is link between malicious node and destination which is of shortest path even then the malicious node will drop the packet and if there is no link between them and it gives false statement of having shortest path to destination even then it will drop the data packets.

B. Solution

In order to detect the malicious node we had slightly enhanced the AODV protocol working. In our approach, when sender broadcast the RREQ packet, it will wait for reply. Following are two things that are required in each node.

1-Reply table
2-Blacklist table

In Reply table, the incoming replies are stored and the route is selected which has highest destination sequence number. Once the route is selected, the sender starts sending dummy packet to its intermediate node. If the intermediate node is normal node, it will forward the packet to destination or its next hop. After some time it will send Conformation Acknowledgment Request to destination via alternative optimal route for conforming whether it has received dummy packet or not. If the destination has received the dumpy packet, it will send Conformation Acknowledgement Reply in form 0 or 1. 0 means destination did not received the dummy packet and 1 means the destination has received the packet. It will ignore the Conformation Acknowledgement Reply from that node to which dummy packet was sent. Based on the reply, the sender will come to know about reliability of its next node whether it is malicious or not.

In Blacklist table, each node will check its table to identify whether the packet is coming from malicious node. If this is true, it will discard the packet. Also when any node identifies the malicious node, it will send alarm packets to the entire network about the malicious behaviors of the node thereby removing the node from routing table and adding it in the blacklist table.

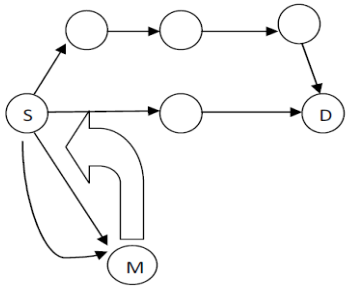


Figure 4. Propagation of dummy packet to M

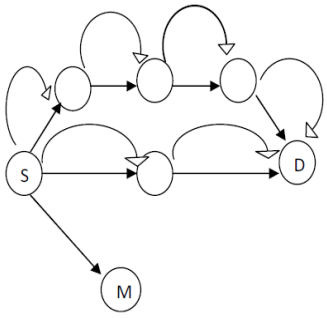


Figure 5. Propagation of CARREQ

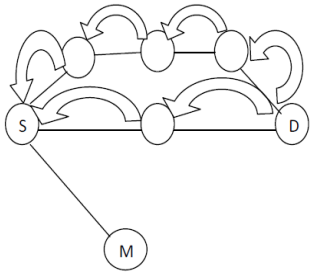
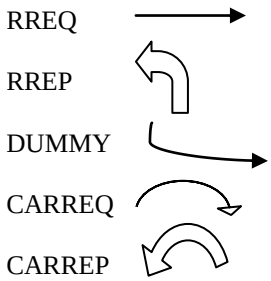


Figure 6. Propagation of CARREP

Proc. of the Second Intl. Conf. on Advances in Electronics, Electrical and Computer Engineering -- EEC 2013

ISBN: 978-981-07-6935-2



VI. Conclusion

In this paper the routing security issues of MANETs are discussed and proposed a solution to detect black hole attack that degrades the performance of network and drop the data packet by giving false reply about having shortest route to destination node. The proposed solution can be useful in detection of black hole node and finding securing path from source to destination. As future work, we intend to develop the simulation of our proposed methodology to evaluate its performance.

Acknowledgment

I would like to take the opportunity to thank people who guided and supported me during this process. Without their contributions, this work would not have been possible. I have a great pleasure in expressing my deep sense of gratitude and indebtedness to Dr. Krishan Kumar Saluja, my supervisor for their continuous guidance and invaluable suggestions at all the time during the research work.

References

[1] C. E. Perkins, E.M. Royer , "Ad-hoc on-demand distance vector routing," Mobile Computing Systems and Applications, 1999. Proceedings ,WMCSA '99. Second IEEE Workshop on, pp.90-100, 25-26 Feb 1999.

[2] C. E. Perkins, E.M.B .Royer, S. Das , "Ad hoc on-demand distance vector (AODV) routing," IETF Internet Draft, MANET working group, Jan.2004.

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

[4] B. Sun, Y. Guan, J. Chen and U. Pooch," Detecting Black-hole Attack in Mobile Ad Hoc Networks". Paper presented at the 5th *European Personal Mobile Communications Conference*, Glasgow, United Kingdom, and 22-25 April 2003.

[5] S. Ramaswamy, H. Furong, M. Sreekantaradhya, J. Dixon and K. Nygard ," 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.

[6] M. Al-Shurman, S. Yoo and S.Park, "Black hole Attack in Mobile Ad Hoc Networks", *ACM Southeast Regional Conference*, pp. 96-97, 2004 (ACM-SE'42), Huntsville, Alabama, 2-3 April 2004.

[7] L. Tamilselvan and Dr. V.Sankaranarayanan, "Prevention of Black hole Attacks in MANET", The 2nd*International Conference on Wireless Broadband and Ultra Wideband Communications, IEE,* 2007.

[8] H. Weerasinghe, H. Fu,"Preventing Cooperative Black Hole Attacks in Mobile Ad Hoc Networks: Simulation Implementation and Evaluation". Paper presented at the *Future Generation Communication and Networking*, Jeju-Island, Korea, 6-8 December 2007.

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

[10] M. Medadian, A. Mebadi, E. Shahri, "Combat with Black Hole attack in AODV routing protocol", Communications (MICC), 2009 *IEEE* 9th *Malaysia International Conference*, pp.530-535, 15-17, Dec.2009.

[11] N. Mistry, D.C. Jinwala, M. Zaveri, "Improving AODV Protocol against Blackhole Attacks", *Proceedings of the International Multi Conference of Engineers and Computer Scientists* 2010 Vol 2, IMECS 2010.

[12] M.Y. Su, Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection systems. *Computer Communications*,*34*(1), pp.107-117,*2011*

[13] K. Liu, J. Deng, "An Acknowledgment Based Approach for the Detection of Routing Misbehavior in MANETS, *IEEE Transaction in Mobile Computing*, Vol. 6, Vol. 5, pp.536-550, May 2007.

About Author (s):

Shashi Gurung has completed his B.Tech from PTU university in 2011.Now he is pursuing M.Tech cse(Networking) from Punjab Institute of Technology (PTU main campus)

Aditya Kumar has completed his B.Tech from PTU university in 2011.Now he is pursuing M.Tech cse(Networking) from Punjab Institute of Technology (PTU main campus)

Krishan Kumar has done BTech computer science and engineering from National Institute of Technology NIT, Hamirpur in 1995. He finished his MS software systems from BITS Pilani in 2001. Recently in 2008, he finished his PhD from Department of Electronics and Computer Engineering at Indian Institute of Technology, Roorkee. Currently, he is an associate professor at SBSSTC Ferozepur, India