IJCSE International Journal of Computer Sciences and Engineering Open Access
Review Paper Vol.-6, Issue-8, Aug 2018 E-ISSN: 2347-2693

Detection and Prevention of Wormhole & Black Hole Attacks in MANET Using AODV Protocol: Review

R.Sharma[1*], R.Thakur[2]

[1*]Dept. of CSE, Maharaja Agrasen University (MAU), Baddi, India
[2]Dept. of CSE, Maharaja Agrasen University (MAU), Baddi, India

**corresponding Author: rmoudgil16@gmail.com*

Available online at: www.ijcseonline.org

Accepted: 12/Aug/2018, Published: 31/Aug/2018

***Abstract*—** Mobile ad-hoc networks are the self-configuring mobile nodes which are connected through the wireless links with the decentralised networks. The nodes in MANET communicate with each other on the basis of mutual trust. Nodes dynamically form a temporary network and are protected using many firewalls and encryption software. But number of them is not sufficient and effective. So the main aim is to provide security services such as authentication, confidentiality, integrity, availability etc. to the mobile users. In this paper the effect of Black hole attack and Worm attack is analysed on the AODV routing protocol in MANET and prevention mechanism is presented to secure the network.

***Keywords*—** MANET, Wormhole Attack, Collaborative black hole Attack, Security, AODV

I. INTRODUCTION

A mobile ad hoc network (MANET), also called as wireless ad hoc network (WANET) is a network that has many free or autonomous nodes, like mobile devices or other mobile pieces that can arrange themselves in different ways [1]. Each node in MANET acts as router that forwards data packet to other nodes. Due to some fundamental characteristics like multi-hop routing, open medium, dynamic topology and distributed cooperation MANETs are vulnerable to various types of attack, such as active and passive attack [2]. In Wormhole attack, an attacker records packets at one location in network and tunnels them to another location [3]. In Collaborative Black hole attack, more than one malicious node act as Black hole to attract all the traffic in network, where all incoming data packets are silently dropped by giving false acknowledgement to source [4].

This paper presents the detection and prevention of Wormhole attack and Collaborative Black Hole attack on MANET using AODV routing algorithm. Ad hoc On-demand Distance Vector (AODV) is reactive routing protocol [5]. In AODV each node maintains a routing table that contains information about reaching destination nodes.

This paper is organised in following manner. Section I starts with the general introduction of MANET, Wormhole and Black hole attack. Section II contains the working of Wormhole and Black hole attack with the help of AODV routing protocol. In Section III we review different methods for detection and prevention of collaborative black hole attack and wormhole attack in AODV based routing Ad-Hoc networks. Section IV concludes the review work with future directions.

II. WORMHOLE ATTACK AND COLLABORATIVE BLACK HOLE ATTACK

A. *Wormhole Attack*

Wormhole attack is a kind of replay attack and is most severe attacks of MANET [6]. Even if, the routing information is confidential, encrypted or authenticated, it can be very effective and damaging [7]. Wormhole attack is basically a Co-operative attack because there is a need of two attacker nodes which will act in co-operation. Generally, two or more attackers are connected via a link called wormhole link. The two malicious nodes in the network are located in such a way that one near to the source node and another near to the destination node thus bypassing information from source node to destination node and destroy the proper routing. Without increasing the hop-count value, an attacker can tunnel a route request packet (RREQ) directly to the destination node. Thus it prevents from discovering any other routes. It may badly disrupt communication, as AODV would be unable to find routes longer than one or two hops. It is easy for the attacker to make the tunnelled packet arrive faster and with better metric value than a normal multi-hop route value. Wormhole attack usually have two malicious nodes [8] shown as X and Y in Fig. 1.

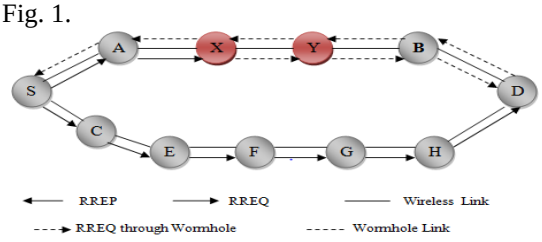

Fig. 1 Wormhole Attack

Both X and Y are connected through wormhole link and attacks the source node S. S broadcasts route request (RREQ) packet to a destination node D during path discovery process. Then, both A and C neighbours of S, receive RREQ and forward RREQ to their neighbours. Now, malicious node X receives RREQ forwarded by A. It records and tunnels the RREQ through wormhole link to another malicious node Y. Y forwards RREQ to its neighbour B. Then finally, B forwards it to destination D. Thus, RREQ is forwarded via S-A-X-Y-B-D. Also on the other hand, RREQ packet is also forwarded through the path S-C-E-F-G-H-D. As X and Y are connected through a tunnel, RREQ from S-A-X-Y-B-D reaches first to D. Therefore, destination D ignores the RREQ that reaches later and select D-B-A-S to unicast a route reply (RREP) packet to the source node S which results into the selection of route S-A-B-D to send data that passes through X and Y malicious nodes that are properly placed as compared to other nodes in the network. Thus, a wormhole attack is not that difficult to set up, but still can harm the MANET.

B. Collaborative Black hole Attack

In collaborative black hole attack, multiple malicious nodes wait for its neighbour to send a RREQ packet. After getting the RREQ packet, malicious nodes will send fake routing information, claiming that they have an optimal route. Malicious nodes send a fake RREP to source node with a modified higher sequence number. In this case, the source node assumes that malicious nodes are having a shortest route towards destination and will discard all RREP packets generated by other nodes which was having genuine route. Then source node will send data packets through malicious nodes to destination node. Instead of forwarding any packet to the destination node malicious nodes will drop all those packets. This attack is called black hole as it drops all data packets. In Fig. 2, S and D are assumed to be source and destination nodes respectively.

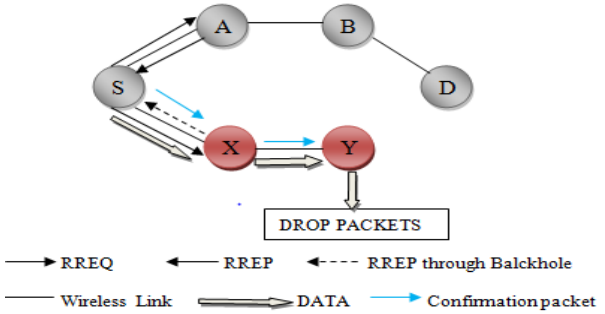

Fig. 2 Collaborative Black hole Attack

Let X and Y are the malicious nodes. When source node wants to send data or communicate with destination node then, S will broadcast a RREQ that is received by the nodes A and X being the neighbours of node S [9]. In collaborative attack, multiple black hole nodes are acting in co-ordination with each other. S receives RREP from X along with the next hop (Y) information. Whenever Y is asked by the source for verification of route to destination through it, it will respond in conformity while in actual it does not have any the route. Hence S will reject all RREP from other nodes and will start sending data packets to destination node D through malicious nodes X and Y. These malicious nodes will drop the all incoming packets from source node.

III. DETECTION & PREVENTION OF ATTACKS

In this section we review different methods for detection and prevention of collaborative black hole attack and wormhole attack in AODV based routing Ad-Hoc networks.

A. DRI table

To keep track of past routing experience among mobile nodes in the network the use of DRI (Data Routing Information) is used [10]. DRI crosschecks the RREP messages from intermediate nodes by source nodes to identify the collaborative black hole nodes and utilize the modified AODV routing protocol to achieve this methodology [11]. Here every node needs to maintain an extra DRI table where, 1 represents true and 0 represents false. In TABLE I each node has two fields called from and through which means for information on routing data packet from the node and through the node respectively.

Table 1. DRI Table

Node ID	Data Routing Information	
	From	Through
3	0	0
5	1	1

In Table 1, the entry 1 1 implies that node 1 has successfully routed data packets from or through node 5, and the entry of 0 0 means that node 1 has not routed any data packets from or through node 3 [12]. The procedure is that the source node sends RREQ to each node, and sends packets to the node which replies the RREP packet. The intermediate node transmits next hop node and DRI table to the source node, and then the source node cross checks its own table and the received DRI table to determine the intermediate node's honesty. After this source node sends the further request to intermediate node's next hop node for asking its routing information, including the current next hop node, the next hop node's DRI table and its own DRI table. Then finally, the source node compares the above information by cross checking to detect the malicious nodes in the routing path and prevent it.

Advantage: Discovery of secure paths from source to destination that avoid collaborative black hole nodes acting in cooperation.

Disadvantage: This method works very slowly if there is not any attack in network and mobile nodes have to maintain an extra database of past routing experiences which results in wastage of memory space.

B. Merkle Tree Method

Merkle tree is a binary tree in which each leaf node contains a hash value and intermediate nodes uses that leaf nodes hash values to create a new combined hash [13].

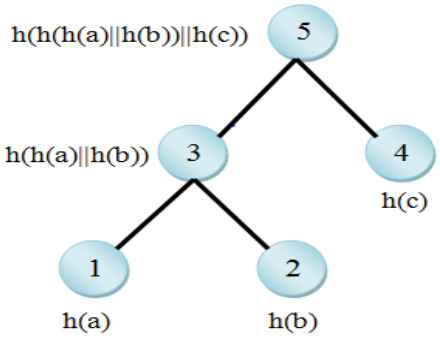

Fig. 3 Merkle Tree

In Fig. 3 | | is concatenation operator. Value of leaf nodes 1, 2, 4 are h(a), h(b), h(c) respectively & value of the interior node 3 is: h(h(a)||h(b)) which is the hashing result of the concatenation of values of children 1 and 2 [14]. Similarly value of node 5 is h(h(h(a)||h(b))||h(c)). Each node contains a hash value which is combination of nodes id and secure value that only the node knows for detection of black hole attack or wormhole attack. This method can be used in both collaborative black hole & wormhole attack. Source node has concatenation of all hashes of one route to destination in its memory. The procedure of checking hash values is that, each node sends concatenation of its hash and previous nodes in route with RREP packet from destination to source. Source node compares this value with prior saved hash value of this route in its memory and if any differences found, it then informs other nodes about maliciousness of this route. Difference between saved value and new value shows that one node may drops RREQ packets and does not send packets to destination that does not have correct value.

Advantage: All nodes do not monitor each other so lot of energy is not consumed for monitoring.

Disadvantage: If a secure constant value is considered for hash, malicious nodes in the path after a time period can drop packets easily and do not send them to destination.

C. Packet Leashes

This method limit the distance travelled by a packet in a network. In packet leashes there are 2 approaches [15]:

1) *Space (Geographical leashes):* This approach establishes an upper bound on the distance that a packet can travel. To use geographic leashes, each node must know its own location and have loose time synchronization with other nodes. Geographical leashes also enable multiple location detection. Each sender sends its own location and a timestamp with each packet. By comparing these values with its own, a receiver may bound the distance between itself and the sender with the following formula:

$$D_{sr} <= |p_s - p_r| + 2v\,(t_r - t_s + \Delta) + \delta \quad (1)$$

Where p_r is position of the receiver, p_s is position of the sender, tr is time of the receiver , t_s is time of the sender, v is upper bound on the velocity of any node, δ is relative location error and Δ is bound on time synchronization.

2) *Time (Temporal Leashes):* This approach establishes an upper bound on packet's lifetime, which restricts the maximum travel distance. In this all nodes must have tightly synchronized clocks. Maximum clock difference (Δ) between any two nodes must be within a few microseconds. In this approach implementation is with a packet expiration time. Sender calculates the packet expiration time to be sent with each packet:

$$t_e = t_s + L/c - \Delta \quad (2)$$

Where t_e is packet expiration time, t_s is packet sent time, c is propagation speed of wireless signal, L is maximum allowed travel distance; $L > L_{min} = \Delta * c$ Δ is maximum clock difference between 2 nodes. Receiver will accept and process a received packet if and only if the time when the packet is received (t_r) is less than the packet expiration time (t_e).

Advantage: This method can find the pinpoint location of wormhole.

Disadvantage: Can't detect exposed attacks and require special hardware for location.

IV. Conclusion And Future Scope

We study the Collaborative black hole and wormhole attack on routing protocol AODV in MANETs. Collaborative black hole attack is more effective as compared to the wormhole attack because in collaborative black hole attack, attacker forcefully makes himself an intermediate node on a selected route due to which the attacker is almost always able to launch an attack during the communication process whereas in case of wormhole attack the effect of attack is not always very high and highly depends on the position of both the colluding attackers. Also in this paper we introduced the best detection techniques for Collaborative black hole and wormhole attack. Most of detection techniques suffer from overload and low speed, which is a research area for developing a detection system against Collaborative black hole and Wormhole attack. Future work is to find an effective solution for Collaborative black hole attack and Wormhole Attack on AODV protocol. This would also be helpful to avoid overloading and accuracy would further increase.

REFERENCES

[1] J. Gronkvist, A. Hansson, and M. Skold, "Evaluation of a Specification-Based Intrusion Detection System for AODV". 2007.

[2] M. Abolhasan, T. Wysocki, and E. Dutkiewicz "A review of routing protocols for mobile ad hoc networks." Ad hoc networks, Vol.2 (1):pp.1–22, 2004.

[3] Kaur, Er. Sandeep Kaur Dhanda, "Analyzing the effect of Wormhole Attack on Routing Protocol in Wireless Sensor Network", International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 8, August 2013.

[4] B. Bharagava, R. Oliveria, Y. Zhang and N. C. Idika, " Addressing Collaborative Attacks and Defense in Ad Hoc Wireless Networks," In Proc. of 2009 29th IEEE Int. Conf. on Distributed Computing Systems Workshops, pp. 447-450, 2009.

[5] C.E. Perkins and E.M. Royer. "Ad-hoc on-demand distance vector routing". In Second IEEE Workshop on Mobile Computing System and Application, WMCSA 99, pages 90 –100, Feb. 1999.

[6] Lui K.-S., sChiu H.S., "DelPHI: Wormhole Detection mechanism for Adhoc Wireless Networks" Proceedings of the 1st International Symposium on Wireless Pervasive Computing; Phuket, Thailand. 16–18 January 2006.

[7] Viren Mahajan, Maitreya Natu, and Adarshpal Sethi, "Analysis of wormhole Intrusion Attacks In MANETS",IEEE Military Communications Conference,MILCOM. Nov 2008.

[8] Rashid Hafeez Khokhar, Md Asri Ngadi and Satira Mandala, "A Review of Current Routing Attacks in Mobile Ad Hoc Networks", International Journal of Computer Science and Security, Volume-2 Issue-3 pp. 18-29, , 2009.

[9] C. E. Perkins and E. M. Royer, "Ad Hoc On-Demand Distance Vector Routing," In Proc. Of IEEEWorkshop on Mobile Comp. Sys.and Apps. Feb. 1999, pp. 90–100.

[10] S. Ramaswamy, H. Fu, M. Sreekantaradhya, J. Dixon, and K. Nygard, "Prevention of Cooperative Blackhole Attack in Wireless Ad Hoc Networks," In Proc. of 2003 Int. Conf. on Wireless Networks, ICWN'03, Las Vegas, Nevada, USA, 2003, pp. 570–575.

[11] Ramaswamy, S., Fu, H., Sreekantaradhya, M., Dixon, j., and Nygard, K."Prevention of cooperative black hole attack in wireless ad hoc networks". In Proceedings of the International Conference on Wireless Networks, 2003

[12] H. Weerasinghe and H. Fu. "Preventing cooperative black hole attacks in mobile ad hoc networks: Simulation implementation and evaluation. In Future generation communication and networking" (fgcn 2007), volume 2, pages 362–367. IEEE, 2007.

[13] A. Baadache and A. Belmehdi."Avoiding black hole and cooperative black hole attacks in wireless ad hoc networks." Arxiv preprint arXiv: 1002.1681, 2010.

[14] D. Eastlake and P. Jones, "Us secure hash algorithm 1 (sha1)," 2001.

[15] Yih-Chun Hu, Adrian Perrig, David B. Johnson, "Packet Leashes: A Defence against Wormhole Attacks in Wireless Ad Hoc Networks", IEEE 2003.

Authors Profile

Miss. R Sharma pursed Bachelor of Technology from Himachal Pradesh University, Shimla, India in 2013 and Master of Technology from Kurukshetra University, Haryana in 2016. She is currently working as an Assistant Professor in Department of Computer Science and Engineering at Maharaja Agrasen University, Baddi, India. She is currently working in the field of Mobile Ad-hoc Networks, Wireless Sensor Networks, Load Balancing and Network Security.

Miss R Thakur is pursuing Bachelor of Technology from Maharaja Agrasen University, Baddi, India and will be passed in 2020. She is currently working in the field of Network Security, Load Balancing and Mobile Ad-hoc network.

