ISSN No. 0976-5697

Volume 1, No. 3, Sept-Oct 2010

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

A Modified Grayhole Attack Detection Technique in Mobile Ad-hoc Networks

Mangesh M. Ghonge*
Faculty
Department of Computer Science & Engineering
Jawaharlal Darda Institute of Engineering &
Technology, Yavatmal, India

Pradeep M. Jawandhiya
Assistant Professor & Head of Department
Department of Computer Science & Engineering
Jawaharlal Darda Institute of Engineering &
Technology, Yavatmal, India

Abstract: Mobile Ad Hoc Networks are vulnerable to various types of Denial of Service (DoS) attacks for the absence of fixed network infrastructure. The Gray Hole attack is a type of DoS attacks. In this attack, an adversary silently drops some or all of the data packets sent to it for further forwarding even when no congestion occurs. Our proposed scheme comprises two steps of detecting malicious node in the network: Detection of malicious activity, Identification of malicious node. The first step is to detect any malicious activity took place in network or not and second if malicious activity took place in the network then identification of that malicious node.

Keywords: MANET, Security attacks, Grayhole attack

I. INTRODUCTION

An ad hoc network is a collection of nodes that do not rely on a predefined infrastructure to keep the network connected. So the functioning of Ad-hoc networks is dependent on the trust and co-operation between nodes. Nodes help each other in conveying information about the topology of the network and share the responsibility of managing the network. Hence in addition to acting as hosts, each mobile node does the function of routing and relaying messages for other mobile nodes. Early research work on route establishment in MANET has mainly focused on the probability and the efficiency, and assumes nodes are trustworthy and cooperative. Recently, more attention has been given to security problems in MANET

The Gray Hole attack is a kind of Denial of Service (DoS) attacks. In this attack, an adversary first exhibits the same behavior as an honest node during the route discovery process, and then silently drops some or all of the data packets sent to it for further forwarding even when no congestion occurs. The malicious nodes could degrade the network performance; disturb route discovery process, etc. In this paper, we proposed a simple two step method to detect the malicious node in the network and isolate the node from the network.

II. RELATED WORKS

Marti et al [1] proposed to trace malicious nodes by using watchdog/pathrater. This scheme was consisted of two related algorithms: 1) the watchdog algorithm. When a node forwards a packet, the node's watchdog verifies that the next node in the path also forwards the packet. The watchdog does this by promiscuously listening to the next node's transmissions. If the watchdog finds the next node does not forward the packet during a certain period of time, the next node will be suspected as a malicious node. If the next node's tally exceeds a predefined threshold, the watchdog will accuse the next node as a malicious node to the source node; 2) the pathrater algorithm. The source node selects the path that most likely to deliver packets, according to the reports provided by watchdogs equipped with each node in the network. The proposal has two shortcomings: 1) to monitor the behavior of nodes two or more hops away, one node has to trust the information from other nodes, which introduces the vulnerability that good nodes may be bypassed by malicious accusation; 2) bi-directional communication links are needed. Awerbuch et al [2] proposed to detect malicious nodes by using acknowledgements sent by destination node. This scheme was consisted of three related algorithms:

1) The route discovery with fault avoidance. By using flooding, cryptography algorithms and weight list, the source nodes could discover route that will deliver packets;

2) The Byzantine fault detection. Based on binary search algorithm and the input path, the source node could detect malicious nodes with Byzantine behavior;

3) The link weight management. This algorithm is used to update the link weight. The proposal has three shortcomings: 1) the bandwidth overhead is significant, as the destination node will send an acknowledgement whenever it receives a packet; 2) it is a challenging work to make sure that the source node has a shared key with each node in the network; 3) the probe packet is easily to be distinguished from other general packet, as the probe packet contains a probe list. Just el al [3] have reviewed the related works on tracing packet dropping nodes, and proposed to detect malicious nodes by using the probe technique. This scheme was consisted of three related algorithms:

1) The probing path selection algorithm. This algorithm is used to select the probing paths;

2) The probing algorithm. This algorithm is used to detect possible malicious nodes in the probing path; the diagnosis algorithm. This algorithm is used to test the possible malicious nodes by using the property of bi-directional communication link.

The proposal has four shortcomings: 1) the source node will begin to probe malicious nodes when it finds that Gray Hole attack has taken place. On considering the dynamic topology of MANET and the random behavior of malicious nodes, this method is not satisfying; 2) bi-directional communication links are needed; 3) the efficiency of this method is related to the location of the malicious nodes in the source route; 4) in order to keep malicious nodes from distinguishing probing packets, the probing packets must be encrypted. Huang el al [4] proposed to detect malicious nodes based on one-way hash chain and one-time hash tag commitment. The basic idea of this scheme was as follows:

1) Each packet sent by the source nodes includes an element in the one-way hash chain, an oneway hash tag commitment of the destination node, and a commitment of the next packet;

2) Each intermediate node verify the previous one-way hash chain element with the current one-way hash chain element, and verify the one-way hash tag commitment with the response provided by the destination node;

3) Each intermediate node will monitor the behavior of its succeeding node, and reports the link state to the source node in an encrypted manner.

The proposal has three shortcomings: 1) the bandwidth overhead is significant, as each participant will create/forward acknowledgement; 2) it is a challenging work to distribute a shared secret between each pair of nodes; 3) the source node has to include a commitment on the next packet in the current packet. Papadimitratos el al [9] proposed to realize secure message transmission by using the redundancy of multi-path routing and threshold secret sharing. Because this protocol operates in an end-to-end manner, this method could not detect malicious nodes.

III. AODV PROTOCOL OPERATION

One category of routing protocols categories in ad hoc networks called reactive routing protocols. The reactive routing protocols (e.g. AODV) create routes and maintain them only if these are needed. (Called on demand routing protocols) they usually use distance-vector routing algorithms and in these kinds of protocols see end-toend delay in these kinds of protocols. AODV protocol uses traditional routing tables. This means that for each destination exist one entry in routing table and uses sequence number, that this number ensure the freshness of routs and guarantee the loop-free routing.

This protocol is based on two phase:

1) Route discovery

2) Maintenance route

These phases don't do any task until the network needs to establish a route between source and destination. If the node has no route entry for the destination, the RREQ message (Route Request message) will be broadcasted. In this time, if the next node is the destination, or has a valid route to the destination, a RREP message (Route Reply message) will be generated and sent back to the source. All nodes monitor their own neighbourhood when a node in an active route gets lost. A route error message (RERR message) is generated to notify the other nodes.

IV. A PROPOSED SCHEME

Our proposed scheme comprises two steps of detecting malicious node in the network.

A. Detecting of malicious activity

B. Identification of malicious node

A. Detecting of malicious activity

In order to find out malicious node, both source node and intermediate nodes need to store some information on forwarded messages.

Notation:

Intermediate Node receives message: (ROUTE, TYPE, Nseq, Mi) where ROUTE is the source route, TYPE is the type of the message, Nseq is the sequence number of the session, and Mi is the data part of the message.

Intermediate Node sends ACK message: (ROUTE, TYPE, Nseq, Ni) where ROUTE is the source route, TYPE is the type of the message, Nseq is the sequence number of the session, and Ni is the identity of the node.

Assume there is an active route between source node S and destination node D using the intermediate nodes say A, B and C. Now when Source node S forwards any packet for Destination D through intermediate nodes A, B and C, all these nodes will send back an ACK of packet to its source node S.

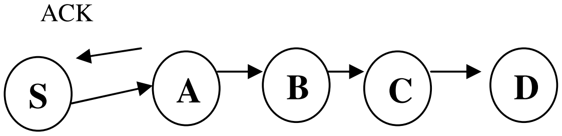

Figure 1: ACK of Packet Send by Intermediate Nodes

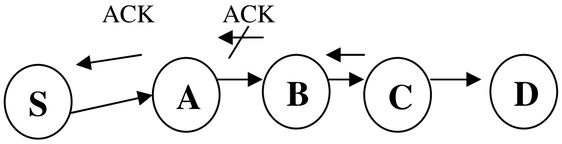

Figure 2: ACK of Packet Not Send by Intermediate Node B

For example if at first step source node forwards a packet to A, it will send back an ACK packet to source node S. Further when packet will reach at B, it will also send back an ACK packet to Source node S through A. Now suppose at some instance, when packet reaches at B and it did not send back an ACK packet to its source node S or it send back its ACK packet to A but it did not further send it to source node as shown in figure 2.

According to this proposed solution, each node has to wait till all ACK packets receive with next hop details from the neighboring nodes. After receiving the first ACK packet, each node sets timer in the 'TimerExpiredTable', for collecting the all ACK from all neighboring nodes. The time for which every node will wait for all ACK is proportional to its distance from the node. And each node calculates the 'timeout' value based on arriving time of the first ACK. After the timeout value, node declares the malicious activity in the network. So source S will send again its packet for Destination D after a specific time but if again this activity was observed, Source node will broadcast a packet to declare the malicious activity in the network and comes to know that one of its intermediate nodes is misbehaving.

B. Identification of malicious node

Upon detection of malicious activity in the network by one of intermediate node, the next step will identify that exactly which intermediate node is doing this activity. Since a malicious activity have already been observed in the network. All the nodes in the network also maintain a list of all nodes in network. So if Node Ni refuses to provide the ACK of forwarding evidence, we will accuse it of a malicious node. Thus upon receiving broadcast packet all the neighbors will cancel their transmission with that particular node and enter this node into the list of misbehaving nodes.

Benefits of Scheme

The benefit of this scheme is that we already know that there is some malicious activity took place in the network while other nodes were observing the number of packet coming into and going out from nodes. If we do not observe malicious activity first, then there can be a situation in which any node which may be a malicious node, can broadcast a packet declaring any legitimate node as malicious node but through detecting malicious activity first we already know that there is some malicious activity took place in the network.

V. CONCLUSION AND FUTURE WORK

This paper presents initial work in detecting misbehaving activity and nodes from MANETs. Currently we are working on its simulation in NS2 to show the results and effectiveness of our solution on AODV.

VI. REFERENCES

[1] S. Marti, T.J. Giuli, K. Lai, and M. Baker. Mitigating Routing Misbehavior in Mobile Ad Hoc Networks. In Proceedings of the Sixth Annual ACM/IEEE International Conference on Mobile Computing and Networking (MOBICOM 2000), August 2000.

[2] B. Awerbuch, D. Holmer, C. Nita-Rotaru, and H. Rubens. An On-Demand Secure Routing Protocol Resilient to Byzantine Failures. In ACM Workshop on Wireless Security (WiSe), September 2002.

[3] M. Just, E. Kranakis, and T. Wan. “Resisting Malicious Packet Dropping. In Wireless Ad Hoc Networks.” In Proc. ADHOC-NOW, Oct. 2003.

[4] Q. Huang, IC Avramopoulos, H Kobayashi, B. Liu. “Secure data forwarding in wireless ad hoc networks”. Communications, 2005. ICC 2005. 2005 IEEE International Conference on, Vol. 5 (2005), pp. 3525-3531 Vol. 5.

[5] Gao Xiaopeng Chen Wei,” A Novel Gray Hole Attack Detection Scheme for Mobile Ad-Hoc Networks”, 2007 IFIP International Conference on Network and Parallel Computing – Workshops, pp. 209-214.

[6] Latha Tamilselvan and Dr. V Sankaranarayanan, “Prevention of Blackhole Attack in MANET”,The 2nd International Conference on Wireless Broadband and Ultra Wideband Communications (AusWireless 2007).

[7] Muhammad Zeshan, Shoab A.Khan, Ahmad Raza Cheema, Attique Ahmed,”Adding Security against Packet Dropping Attack in Mobile Ad hoc Networks”, 2008 International Seminar on Future Information Technology and Management Engineering,2008 IEEE.

[8] I Chlamtac, M Conti, et al. “Mobile Ad hoc Networking: Imperatives and Challenges”. Ad hoc Net works, 2003, 1(1):13-64.

[9] YC Hu and A. Perrig. “A Survey of Secure Wireless Ad Hoc Routing”. In IEEE Security and Privacy, vol. 2(3), pp. 28 – 39, May 2004.

[10] S. Marti, T.J. Giuli, K. Lai, and M. Baker. Mitigating Routing Misbehavior in Mobile Ad Hoc Networks. In Proceedings of the Sixth Annual ACM/IEEE International Conference on Mobile Computing and Networking (MOBICOM 2000), August 2000.

[11] B. Awerbuch, D. Holmer, C. Nita-Rotaru, and H. Rubens. An On-Demand Secure Routing Protocol Resilient to Byzantine Failures. In ACM Workshop on Wireless Security (WiSe), September 2002.

[12] M. Just, E. Kranakis, and T. Wan. “Resisting Malicious Packet Dropping. In Wireless Ad Hoc Networks.” In Proc. ADHOC-NOW, Oct. 2003.