Indian Journal of Science and Technology, *Vol 9(4), DOI: 10.17485/ijst/2016/v9i4/77755, January 2016*
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

A Khattak Approach for Detection and Removal of Black and Gray Hole Attacks in MANET

K. Hizbullah*, U. Arif Iqbal and Insafullah

Department of Information Techonolgy, Hazara University Mansehra, Pakistan; hizbullahkhattak@yahoo.com, drarif@hu.edu.pk, insafktk@gmail.com

Abstract

Mobility of nodes and dynamic changing topology creates security issues in MANETs making it vulnerable to some prominent attacks. Black and gray hole attacks drop the data packets in AODV. In this paper we propose a technique to detect and isolate malicious nodes. A cost effective Hash function to compute Message Digest (MD) is used for secure data transmission and data integrity in AODV. Malicious node is detected with the identification number or hop count. The security analysis of the existing ADOV and modified AODV is discussed. On the basis of analysis, we conclude that the proposed AODV is more secure as it provides cost effective secure mechanism for data transmission.

Keywords: Black and Gray Hole Attacks, Hash Function, Identification Number, MANETs, Message Digest

1. Introduction

MANETs is a set of wireless nodes that can be dynamically setup without any pre-existing network infrastructure. Mobility of nodes and dynamic changing topology in AODV makes the routing jobs more interesting and challenging for the researchers. In this network, each and every node acts as a router for routing the data packets to the destination[1]. This network is used in military operations, emergency relief operations and terrorism response[2]. Due to lack of centralized administration, mobiles nodes can freely move inside or leave the network that makes this network vulnerable to various kinds of attacks[3]. Different malicious nodes can easily become part of the network for disrupting the secure data packets transmission.

In this paper we propose a technique for detection and removal of two prominent attacks i.e., black and gray hole attacks which discards the data packets in AODV. Black hole node replies to all Route Request (RREQ) messages fallaciously claiming that it has the freshest enough route to the destination and thus redirects all data packets in the network towards its own and later on drops the entire data packets. In gray hole attacks, malicious node becomes a part of the network in similar way but in gray hole attack malicious node first work as an honest node by sending some of the data packets and later on starts dropping some or all the data packets[4]. It is hard to find out and isolate gray hole attack because it sends data partially.

We propose a technique for detection and isolation of malicious node. Our proposed approach is a slight modification of the existing AODV. Before sending the data packets, we compute a Message Digest (MD) of the message by applying a hash function over the entire message. Source broadcast this MD in the RREQ message to destination.

After receiving this route request message an intermediate node having a freshest path to destination sends back the (RREP) message with addition of providing his identification number (hop count) to source node. Simultaneously, intermediate node forwards (RREQ) message to destination with addition of providing his identification number (hop count).

**Author for correspondence*

After receiving this RREQ message from the intermediate node, destination node waits for getting another RREQ message from any other node. After receiving second RREQ message it compares the two MDs, if they are equal it means it got the correct MD form the intermediate node.

When destination node receives complete message from the source, it applies hash function on the message to recompute the message digest. Destination node compares this MD with the one it received earlier from the source. If both theses two computed MDs are same, it means data have been received secure. If they are different, it means data have been discarded by that malicious node. In this case it broadcast about that malicious node in the network and inform the source to re-establish route for sending the data. After receiving the alarm message all the nodes blacklist this malicious node in the network.

The rest of the paper is organized as follows. Section 2 presents the related work. Section 3 introduces the proposed network model. Section 4 discusses the security analysis and Section 5 discusses conclusion and future work.

2. Related Work

Detections and avoidance of AODV from these prominent attacks have been a hot area of research for the researcher and many researchers have proposed various kinds of techniques for preventing of AOV from these attacks. Some of them have discussed as such;

In SAODV[5] technique, when source receive RREP packet, it sends SRREQ packet to destination for the verification of a secure route. SRREQ packet contains a secret code that is randomly generated. When destination receives at least two such packets, it sends back SRREP packets to source. This SRREP packet also contains a secret code that is randomly generated by the destination. After receiving at least two such packets, source selects the shortest route that is considered a secure for data packets transmission. The limitation of this scheme is that it increases the delay and as a result throughput gets increase.

In wait and check strategy[6] for avoiding black hole attack. Source node waits for collecting RREP messages from other neighbors' nodes. After receiving the first RREP message, source set a time for collecting other RREP messages. Source node stores the packets sequence number and it's receiving time in a collect route reply table. Route is checked and verified on the receiving time of the first RREP packet and the already set threshold time value. The wait strategy creates additional delay.

In[7] technique of introducing a kind of data structure, a trust table at all nodes is proposed. The table contains the addresses of trustworthy nodes. One extra field in the RREP packet has been added that shows the reliability of the node. Source node send the data in case of RREP is delivered from a reliable node if not it waits for more RREPs. The drawback of this solution is creating delay.

In[8] a technique of DPRAODV is presented. In this scheme one check is added for finding whether the sequence number of RREP is larger than the threshold value. Node is considered malicious if threshold value is lesser than the sequence number of RREP. After identification of an attacker node an ALARM message is sent to its neighbour node and it contains black list node as parameter. Afterward when any node gets RREP packet, it verifies this node in its list of black list nodes. If this node is black listed, it does not receives replies from that node. The limitation of this scheme is that it increases the overhead and delay.

3. Proposed Solution

Our proposed technique is the modification of existing AODV routing protocol at different level. In AODV routing protocol source node broadcasts a RREQ message in the networks for finding a shortest route to the destination. When destination node or any intermediate node having freshest enough route with destination receives this RREQ message, it replies back to the source with RREP message and this way the route finding procedure is completed. In Figure 1, node H is replying back to the source S that it has the freshest enough route with destination node D.

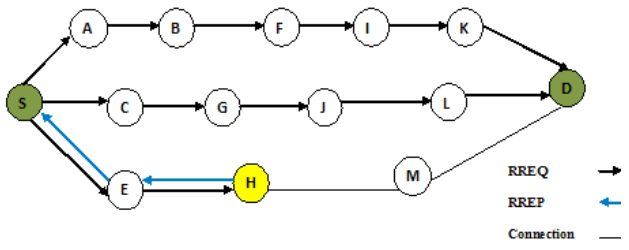

Figure 1. AODV RREQ and RREP messages.

In our proposed AODV, source node applies a hash function on complete message to get a unique Message Digest (MD) before sending RREQ message to destination.

$$H(M) \rightarrow MD$$

When source broadcasts a RREQ message in the networks for finding the shortest route to destination, it appends computed Message Digest (MD) with (RREQ) message as shown in the Figure 2.

Any intermediate node when receives this route request and message digest (RREQ+MD) message, it replies back to source node with Route Reply (RREP) message with providing his identification number which in this case is his hop count. At the same time, the message of RREQ+MD that it receives earlier sends to the destination with the addition of his identification number (Hop Count). In the Figure 2, node H has been mentioned as a malicious node that replies to source node informing that it has the freshest node to the destination. When the malicious node sends this RREP+Hop Count Message to its neighbor node it checks whether his own hop count is one less than this hop count number.

If ($HC_{rep\ node}$ == $HC_{next\ neighbor\ node}$ + 1)

then

send RREP + HC → next neighbor node or source node

else

send $HC_{malicious\ node}$ → source node

This is just to verify that malicious node may have not provided the wrong hop count information.

After receiving this route reply (RREP+Hop Count) message, source stores this identification number in its Table 1.

On the other side, when destination node receives this Route Request and Message Digest message (RREQ+MD), it stores this MD in its table. Destination node waits to receive second route request (RREQ+MD) message from

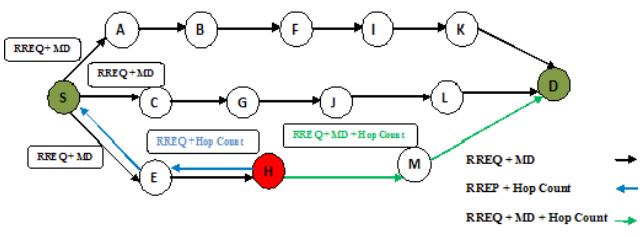

Figure 2. Proposed AODV.

Table 1. Source node

RREP Hop Count
2

Table 2. Destination node

RREQ Hop Count	Hash
2	MD

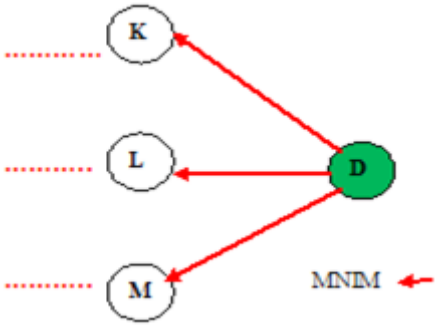

Figure 3. Malicious Node identification message to source.

any other node and when it get the second (RREQ+MD) message it compares second MD with the one that has provided earlier by the replier node.

If ($MD_{rep\ node}$ = = $MD_{other\ node}$)

wait → data packets

else

broadcast alarm msg

This is shown in the Figure 3.

In case of correct MD the destination node waits for receiving the data packets for a specific threshold time value. If destination node does not receive data packets during this time, it broadcast the malicious node identification message in the network.

After receiving all the data packets, destination node applies hash function on the received message to recompute the Message Digest (MD) and then compares this with the stored one it receive at the beginning. If both MDs are same it means all the data packets have arrived secure and if different it means some data packets have been lost. In this case, it broadcast the malicious node identification message in the network to blacklist it for no further communication with it. Source node also blacklists this node and re-establishes the route from the beginning.

4. Security Analysis

The proposed protocol has the advantages of both identifying and removing of malicious nodes. Furthermore, proposed scheme uses a hash function for data integrity to make AODV more secure and reliable. The proposed protocol identifies the malicious node with just addition of sending node identification in the RREQ packet to the destination. Later on it uses a hash function that is more cost effective technique than any cryptographic scheme for ensuring the data integrity. Most of the researcher have proposed their techniques either for just identifying the malicious node or for making AODV secure but our techniques provides both these functions.

Therefore, our proposed technique is more reliable for the detection and removal of malicious node and with better provision of security scheme of data integrity.

5. Conclusion

In this paper, a technique for the detection and removal of malicious node has been presented. In addition, the proposed technique has also a solution for data integrity as well as. This technique is more efficient and reliable for both the detection/removal of malicious node and for data integrity. In future the proposed technique will be simulated to measure different metrics like delay, overhead, throughput, packet delivery ratio etc.

6. References

1. Anchugam CV, Thangadurai K. Detection of black hole attacks in mobile ad-hoc networks using ant colony optimization-simulation analysis. Indian Journal of Science and Technology. 2015 Jul; 8(13):1–10.
2. Akhtar MAK, Sahoo G. Behavior based high performance protocol for MANET. Indian Journal of Science and Technology. 2013 Oct; 6(10):5342–50.
3. Amiri R, Rafsanjani MK, Khosravi E. Black hole detection by invalid IP addresses in mobile ad hoc networks. Indian Journal of Science and Technology. 2014 Apr; 7(4):401–8.
4. Khattak H, Nizamuddin N, Khurshid F, Amin N. Preventing black and gray hole attacks in AODV using optimal path routing and hash. Proceedings of the 10th International Conference on Networking, Sensing and Control; Paris, France. 2013 Apr. p. 645–8.
5. Lu S, Li L, Lam K-Y, Jia L. SAODV: A MANET routing protocol that can withstand black hole attack. Proceeding of the International Conference on Computational Intelligence and Security; Beijing, China. 2009 Dec. p. 421–5.
6. Tamilselvan L, Sankaranarayanan V. Prevention of blackhole attack in MANET. Proceeding of the 2nd International Conference on Wireless Broadband and Ultra Wideband Communications (AusWirless); Sydney, Australia. 2007. p. 21–6.
7. Khamayseh Y, Bader A, Mardini W, Yasein MB. A new protocol for detecting black hole nodes in adhoc network. International Journal of Communication Networks and Information Security. 2011 Apr; 3(1):36–47.
8. Raj PN, Swadas PB. DPRAODV: A dynamic learning system against blackhole attack in AODV based MANET. International Journal of Computer Science Issues. 2009; 1(2):54–9.