A Novel Solution for Grayhole Attack in AODV Based MANETs

Rutvij H. Jhaveri[1], Sankita J. Patel[2] and Devesh C. Jinwala[3]

[1] Computer Engineering Department, Shri S'ad Vidya Mandal Institute of Technology, Bharuch 392-001, Gujarat, India

[2,3] Computer Engineering Department, Sardar Vallabhbhai National Institute of Technology, Surat 395-007, Gujarat, India

{rutusoft@yahoo.com;sjp@coed.svnit.ac.in; dcj@coed.svnit.ac.in }

Abstract. Security plays a vital role to provide protected data transmission in Mobile Ad-hoc Networks (MANETs). Mobile nodes communicate in multi-hop way via routing protocols that work in physically insecure environment. MANETs are susceptible to various Denial-of-Service (DoS) attacks on network layer due to their unique characteristics such as unclear line of defense, limited communication resources, lack of centralized monitoring, wireless radio communication and varying topology. Grayhole attack is a major DoS attack that disrupts data transmission in the network by sending false routing information. To keep the communication route free from such attacks, it is imperative to design a secure and efficient protocol. In this paper, we provide a modification of Ad-hoc On-demand Distance Vector (AODV) protocol to prevent Grayhole attack in which a node sending bogus routing information is detected and recorded by the node receiving it. To avoid the use of extra control packets, default routing packets are given additional responsibility to pass information about malicious nodes. The simulation results in ns-2 show that the solution is reliable against multiple attackers and gives significant improvement in packet delivery ratio with negligible difference in end-to-end delay and routing overhead.

Keywords: MANETs, Security, Grayhole Attack, AODV, R-AODV.

1 Introduction

Role of MANETs has become vital in pervasive computing due to their self-configurable and rapidly deployable nature. A MANET connects mobile devices anytime and anywhere without any fixed infrastructure or centralized access point. To make the ad-hoc network and to stay connected, nodes act as a router to relay packets for peer nodes. In the environment where nodes have limited transmission range and high mobility, routes may change frequently [1]. As a result, routing becomes a major challenge. The duty of establishing and maintaining routes is performed by special routing protocols [2]. Among all routing protocols, AODV is the most popular on-demand protocol. As makers of AODV did not focus on its security aspect, malicious nodes can perform many attacks just by not following the protocol rules. Moreover, in-

herent nature of MANETs make them vulnerable to various kinds of attacks such as spoofing, flooding, eavesdropping, modification of packet contents, routing table overflow, route cache poisoning and DoS attacks viz. Wormhole attack, Sinkhole attack, Grayhole attack and Blackhole attack [3]. In this paper, we focus on security against Grayhole attack that is one of the most dangerous DoS attacks disrupting the basic functionality of AODV of delivering data packets from source to destination and thus, degrading network performance [4].

Grayhole attack is another version of Blackhole attack in which the attacker promotes itself as having a shortest valid route to the destination by sending fabricated routing information [5]. As a result, a bogus route will be created through the malicious node which dumps the received packets for specific time period and behaves normally afterwards. This disturbs route discovery process and absorbs network traffic [4, 6]. Due to the unpredictable nature, detection of Grayhole attack is not an easy task. In this paper, we provide a variation of AODV that detects and removes malicious nodes performing Grayhole attack. The primary objective of designing this routing protocol is to set up shortest secured route with minimal overhead and to consume minimum resources. The protocol adds little functionality to each and every node involved in the session; an intermediate node receiving unusual routing information from RREP (Route Reply Packet) sent by neighbor node considers that node as a malicious node. The intermediate node marks it as malicious node in the routing table and appends its information to the RREP and marks that RREP with do not consider flag; every node receiving that RREP on the reverse path updates its routing table to mark the node as malicious node. Before sending RREQ (Route Request Packet), a list of malicious node is appended to it and every node receiving the broadcasted RREQ marks entries of the listed nodes as malicious in the routing table. Thus, a node finds the attacker either by checking do not consider flag of RREP, by checking the malicious node's entry in its routing table or by identifying fabricated routing information from the received RREP. The solution uses default control packets, RREP and RREQ, to inform other nodes about ignoring the routing packets received from malicious nodes and thus, malicious nodes are isolated.

The remainder of paper is organized as follows. Section 2 presents the related work. Section 3 describes design of our solution to prevent Grayhole attack. Simulation results and analysis are presented in Section 4. Section 5 concludes the paper.

2 Related Work

Vishnu et. al [7] proposed a mechanism that establishes a backbone network of trusted nodes over the ad hoc network. An unused IP address from a backbone node is requested by the source node periodically. During route discovery process, a node sends an RREQ to search the destination node as well as the unused IP. If attacker is present, it sends RREP for the unused IP also. For a positive response to unused IP, source node starts detection process. The mechanism, though, assumes the network is divided into several grids and trusted nodes have powerful battery and high transmission range; it also assumes that a node entering the network is capable of finding its grid location and number of malicious nodes at any point must be less than normal

nodes which may not be likely in several situations. Mamatha et. al [8] provided a mechanism using simple acknowledgement and flow conservation scheme in which one-way hash code is attached to data packets to verify the correct match when the destination node receives the packet. Destination sends CONFIDENTIALITY LOST for erroneous packet received and asks sender to change to another intermediate node to send packets. When destination sends ACK for correct packet received, source node checks if ACK is received within specific time. Due to addition in control packets the mechanism increases routing overhead. Arshad et. al [9] provided a simple approach with passive acknowledgement in which promiscuous mode is used to examine the channel that allows a node to recognize transmitted packets that are irrelevant of the actual destination; next hop node is selected to find the shortest trusted route. A node can confirm that packets it has sent to its neighbor are indeed forwarded. However, instead of observing one node's request, observing overall traffic would have been a better alternative; moreover, due to promicuous mode, the approach has limitations of high energy consumption and more computational overhead. A scheme to fight against packet forwarding misbehavior is addressed by Oscar et. al [10] that works on the principle of flow conservation and accusation of misbehaving nodes. A threshold value is selected to differentiate normal nodes and malicious nodes. However, it is impossible to achieve the average throughput as that of a network where there is no malicious node present because the algorithm needs some time to gather data to identify and to accuse malicious nodes. As a result, malicious nodes can drop packets before being accused and detached from the network during the preliminary phase; it also adds routing overhead due to addition of control packets. Piyush et.al [11] provided a solution in which both source and destination nodes perform secure transfer of data packets by carrying out end-to-end checking. In the case of failure in checking, the backbone network detects malicious nodes. Though, the mechanism works on the assumption that any node in the network has more trusted nodes as neighbors than malicious nodes which may not be the case in many scenarios. Jaydip et. al [12] proposed an algorithm based on threshold cryptography in which nodes collect the data forwarding information of neighbors in a table; node identifies a suspicious node after examining the table and initiates detection procedure using collaborative and distributed algorithm; it informs other nodes about the malicious node using an ALARM packet signed with private key. However, introduction of ALARM packet leads to increase in routing overhead.

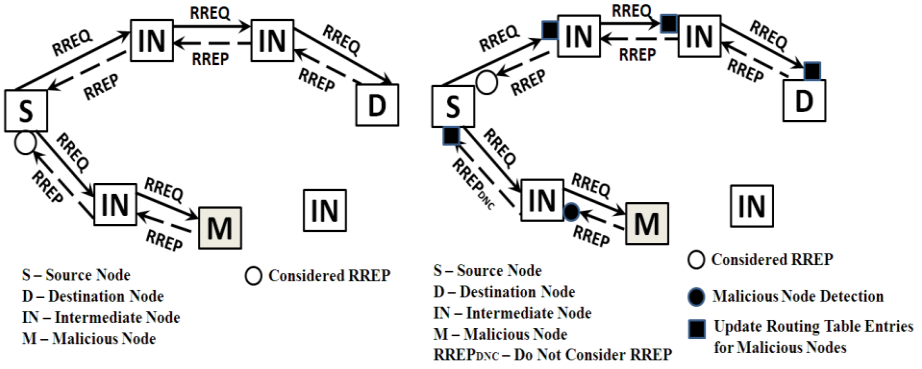
To remove the shortcomings of above solutions, it is imperative to devise a protocol that discovers secured shortest route to destination with minimum possible increase in end-to-end delay and routing overhead. In the following section, we discuss design of our protocol.

3 R-AODV Protocol

Fig. 1(a) shows a MANET using AODV protocol in which a Grayhole attacker M is present. S receives RREP from M with unusually high sequence number in response to broadcasted RREQ; while destination D sends RREP having legitimately higher sequence number. As RREP sent by M contains higher sequence number of all re-

ceived RREPs, S unknowingly selects path through M to transfer data packets and as a result, M drops some of the received packets for a specific time causing denial-of-service in the network.

Our solution, Reliable-AODV (R-AODV), prevents Grayhole attack even when number of malicious nodes are more compared to genuine nodes surrounding a node at any time. Unlike some existing proposals, our solution does not assume promiscuous mode of operation as it cannot be used for mobile nodes with directional antennas; moreover, promiscuous mode leads to more energy consumption along with additional computational overhead [12]. Contrasting some of the existing solutions, we do not introduce extra control packets to propagate information about malicious nodes to other nodes in the network; instead, we assign this functionality to default RREQ and RREP control packets. A PEAK value is computed using number of sent out RREQs, number of received RREPs and routing table sequence number after every received RREP as these three parameters determine the state of a node in an ad-hoc network using AODV protocol; the PEAK value is used to distinguish genuine nodes from malicious nodes acting as genuine nodes. As discussed in [13], a new field called MALICIOUS_NODE is added in the routing table for marking a node as malicious node; a flag called DO_NOT_CONSIDER is added to the structure of RREP to identify reply from a malicious node; a MALICIOUS_NODE_LIST is appended to the structure of RREQ to notify other nodes about malicious nodes in the MANET. Working of R-AODV in the presence of an attacker is shown in Fig. 1(b); an intermediate node IN receiving RREP from malicious node M with sequence number higher than the calculated PEAK value marks that RREP as DO_NOT_CONSIDER and M as MALICIOUS_NODE in the routing table; on the reverse path to S, RREP updates routing tables of INs and S with MALICIOUS_NODE entries for M. When S intitiates route discovery process in future, it appends a MALICIOUS_NODE_LIST to RREQ to inform other nodes about the existence of malicious nodes recorded till time along with M. As a result, replies from all the malicious nodes remain unconsidered and they remain isolated from genuine nodes. We change functionalities of nodes sending RREQ, nodes receiving RREQ and nodes receiving RREP as shown in Fig. 2; while functionalities of nodes sending RREP remain as it is as default AODV.



(a)AODV (b) R-AODV

Fig. 1. Route discovery process in presence of attacker

```
Mobile Node Receiving RREP
If(Node sending RREP is marked as MALICIOUS_NODE in the
ROUTING_TABLE){
Mark RREP as DO_NOT_CONSIDER;
}
Else if (RREP is marked as DO_NOT_CONSIDER) {
Mark the node sending RREP as MALICIOUS_NODE in the
ROUTING_TABLE;
}
Else {
     Calculate PEAK value;
     If (RREP_SEQUENCE_NO > PEAK) {
         Mark it as MALICIOUS_NODE in the ROUTING_TABLE;
         Mark RREP as DO_NOT_CONSIDER;
         Append MALICIOUS_NODE information in RREP;
        }
}
Mobile Node Sending RREQ
If (MALICIOUS_NODE entry exists in the ROUTING_TABLE) {
Make MALICIOUS_NODE_LIST and append it to RREQ;
}
Mobile Node Receiving RREQ
If (Received RREQ contains MALICIOUS_NODE_LIST) {
Mark the nodes as MALICIOUS_NODEs in the ROUTING_TABLE;
}
```

Fig. 2. Design of R-AODV

4 Simulation Results and Analysis

Our simulations are performed using ns-2 (Ver.-2.34) simulation tool [14]. A new routing agent is included in ns-2 containing Grayhole attack. We randomly move 5 to 30 nodes in the area of 800m x 800m for the simulation time of 50 seconds. Transmission range of each node is 250m. Table 1 shows simulation parameters along with values. To analyze the performance of R-AODV, we use the following metrics:

Packet Delivery Ratio (PDR): The ratio of number of data packets received by the application layer of destination nodes to the number of packets transmitted by the application layer of source nodes.

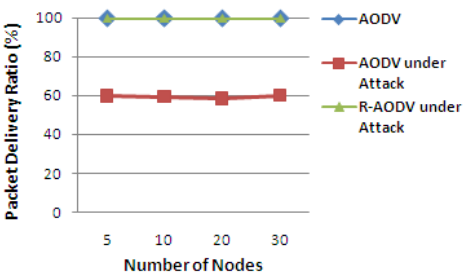
Average End-to-End Delay: Average time taken by transmitted data packets to reach to corresponding destinations.

Normalized Routing Overhead: The ratio of number of routing control packets to the number of data packets.

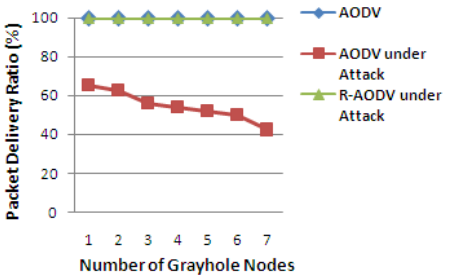
Table 1. Simulation parameters

Parameter	Value
Terrain Area	800 m x 800 m
Simulation Time	50 sec
Traffic Type	CBR (UDP)
Maximum Bandwidth	2 Mbps
Transmission Range	250 m
Data Payload	512 Bytes/Packet
Pause Time	2.0 sec
Maximum Speed	20 m/sec
Number of Nodes	5 to 30
Number of Grayhole Nodes	1 to 7

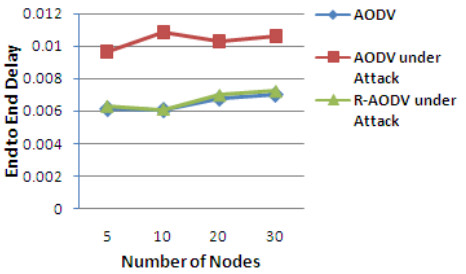
We take ideal scenarios with zero packet loss for AODV to exactly measure the effects of Grayhole attack. Fig. 3 (a) shows the performance of R-AODV under Grayhole attack by varying network size in presence of a single attacker; R-AODV gives tremendous improvement in PDR which is equivalent to that of AODV in normal conditions as far as there is an alternative genuine node present to replace isolated malicious node to establish an alternate secured route. Even when multiple attackers are present, R-AODV proves its reliability by preventing all malicious nodes wishing to involve in data transmission phase. Fig. 3 (b) shows the performance comparison of AODV and R-AODV in presence of multiple attackers for a MANET containing 20 nodes; as the number of attackers increase PDR of AODV decreases, while R-AODV performs equally well and gives significant rise in PDR. Fig. 3 (c) depicts the performance of R-AODV in terms of end-to-end delay by varying network size in presence of single attacker. R-AODV shows remarkable improvement in end-to-end delay in comparison with AODV under attack. Fig. 3 (d) shows the graph comparing normalized routing overhead with increasing number of nodes. In presence of an attacker, R-AODV proves its efficiency with noticable decrease in normalized routing overhead compared to AODV as there is no extra control packets added to R-AODV.



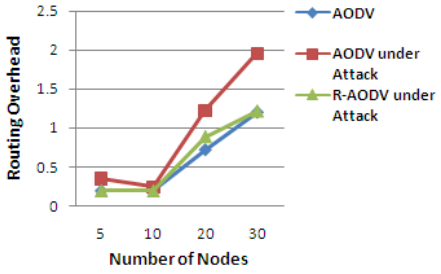
(a) PDR with single attacker



(b) PDR with multiple attackers



(c) End-to-End delay Vs Network size



(d) Routing overhead Vs Network size

Fig. 3. Performance analysis of R-AODV against Grayhole attack

5 Conclusion and Future Work

DoS attacks performing packet forwarding misbehavior have become major security threats for AODV protocol in MANETs. In this paper, we presented an alternative solution for AODV protocol called R-AODV that proves its reliability against Grayhole attack. Under the attack, AODV cannot perform its basic functionality to reliably transfer all data packets to the destination and its performance drops significantly, while R-AODV detects and isolates multiple malicious nodes performing the attack and fulfills its design objectives. This novel solution finds shortest secured route without adding extra control packets and gives nearly the same PDR as default AODV with negligible difference in normalized routing overhead and end-to-end delay. R-AODV is equally applicable to Blackhole attack.

References

1. Nadia Qasim, Fatin Said, Hamid Aghvami: Performance Evaluation of Mobile Ad Hoc Networking Protocols. In: World Congress on Engineering, pp. 219--229 (2008)
2. Payal N. Raj, Prashant B. Swadas: DPRAODV: A Dynamic Learning System against Black hole Attack in AODV Based MANET. In: International Journal of Computer Science Issues, vol. 2, issue 3, pp. 54--59 (2010)

3. Nital Mistry, Devesh C. Jinwala, Mukesh Zaveri: Improving AODV Protocol against Black hole Attacks. In: International Multiconference of Engineers and Computer Scientists, vol. 2, pp. 1034--1039 (2010)
4. Gao Xiaopeng, Chen Wei: A Novel Gray Hole Attack Detection Scheme for Mobile Ad-Hoc Networks. In: IFIP International Conference on Network and Parallel Computing, pp. 209--214 (2007)
5. Rutvij H. Jhaveri, Ashish D. Patel, Jatin D. Parmar, Bhavin I. Shah: MANET Routing Protocols and Wormhole Attack against AODV. In: International Journal of Computer Science and Network Security, vol. 10 No. 4, pp. 12--18 (2010)
6. Anu Bala, Munish Bansal, Jagpreet Singh: Performance Analysis of MANET under Black hole Attack. In: 1st International Conference on Networks & Communications, pp. 141--145 (2009)
7. Vishnu K., Amos J. Paul: Detection and Removal of Cooperative Black/Gray hole Attack in Mobile ADHOC Networks. In: International Journal of Computer Applications, vol. 1, No. 22, pp. 38--42 (2010)
8. G.S. Mamatha, S.C. Sharma: A Robust Approach to Detect and Prevent Network Layer Attacks in MANETS. In: International Journal of Computer Science and Security, vol. 4, issue 3, pp. 275--284 (2010)
9. Arshad Jhumka, Nathan Griths, Anthony Dawson, Richard Myers: An Outlook on the Impact of Trust Models on Routing in Mobile Ad Hoc Networks (MANETs). In: Networking and Electronic Commerce Research Conference (2008)
10. Oscar F. Gonzalez, Godwin Ansa, Michael Howarth, George Pavlou: Detection and Accusation of Packet Forwarding Misbehavior in Mobile Ad-Hoc Networks. In: Journal of Internet Engineering, vol. 2, no. 1, pp. 181--192 (2008)
11. Piyush Agrawal, R. K. Ghosh, Sajal K. Das: Cooperative Black and Gray Hole Attacks in Mobile Ad Hoc Networks. In: 2nd International Conference on Ubiquitous Information Management and Communication, pp.310--314 (2008)
12. Jaydip Sen, N. Girish Chandra, Harihara S.G., Harish Reddy, P. Balamuralidhar: A Mechanism for Detection of Gray Hole Attack in Mobile Ad Hoc Networks. In: 6th International Conference on Information, Communications and Signal Processing, pp.1--5 (2007)
13. Rutvij H. Jhaveri, Sankita J. Patel, Devesh C. Jinwala:A Novel Approach for Grayhole and Blackhole Attacks in Mobile Ad Hoc Networks. In: 2nd International Conference on Advanced Computing & Communication Technologies, pp.556--560 (2012)
14. Kevin Fall, Kannan Varadhan: The ns Manual, http://www.isi.edu/nsnam/ns/doc/