A Novel Approach for GrayHole and BlackHole Attacks in Mobile Ad-hoc Networks

Rutvij H. Jhaveri[1], Sankita J. Patel[2] and Devesh C. Jinwala[3]
[1]Computer/IT Engineering Department, Shri S'ad Vidya Mandal Institute of Technology,
Bharuch 392-001, Gujarat, India
[1]rutusoft@yahoo.com
[2,3]Computer Engineering Department, Sardar Vallabh National Institute of Technology,
Surat 395-007, Gujarat, India
[2]sjp@coed.svnit.ac.in, [3]dcj@coed.svnit.ac.in

Abstract—**Due to wireless communication, dynamic topology, limited resources and lack of centralized administration, MANETs are vulnerable to various types of DoS attacks on network layer. In Grayhole and Blackhole attacks malicious nodes deliberately disrupt data transmission in the network by sending incorrect routing information. It is a challenge to keep the communication route free from such attackers. In this paper, we propose a scheme for Ad-hoc On-demand Distance Vector (AODV) protocol, in which an intermediate node detects the malicious node sending false routing information; routing packets are used not only to pass routing information, but also to pass information about malicious nodes. The proposed scheme not only detects but also removes malicious node by isolating it, to make safe and secure communication.**

Keywords-MANETs, Security, Grayhole Attack, Blackhole Attack, AODV.

I. INTRODUCTION

An ad-hoc network can change its form depending on the work on hand. A MANET is an infrastructure-less network consisting of set of mobile nodes or mobile devices wishing to communicate with each other via shared wireless medium; it does not have any centralized administration and therefore, line of defense is pretty unclear. Each node has limited communication range in the network and it node acts as a router to forward packets to another node. It is rapidly deployable and highly adaptive in nature. Nodes have high mobility and communication is done via radio broadcast medium. Therefore, MANETs are widely used in applications such as military communication by soldiers, automated battlefields, emergency management teams to rescue, search by police or fire fighters, replacement of fixed infrastructure in case of earthquake, floods, fire etc., quicker access to patient's data from hospital database about record, status, diagnosis during emergency situations, remote sensors for weather, voting systems, sports stadiums, mobile offices, vehicular computing, electronic payments from anywhere, education systems with set-up of virtual classrooms, conference meetings, peer to peer file sharing systems [1]. The characteristics of MANET along with mobility and radio broadcast medium leads to some major issues for MANETs such as IP addressing, radio interference, routing protocols, power constraints, security, mobility management, service discovery, bandwidth constraints, Quality of Services (QoS), etc. [2]. Among all research issues, though, one of the essential research issues in MANETs is security; Denial-of-Service (DoS) attacks are a major class of threat today.

Two of the most common DoS attacks are Grayhole and Blackhole attacks in MANET. In Blackhole attack, the malicious node generates and propagates fabricated routing information and advertises itself as having a valid shortest route to the destined node [3]. If the malicious node replies to the requesting node before the genuine node replies, a false route will be created. Therefore, packets do not reach to the specified destination node; instead, the malicious node intercepts the packets, drops them and thus, network traffic is absorbed [4]. Grayhole attack is an extension of Blackhole attack in which a malicious node's behavior is exceptionally unpredictable. A node may behave maliciously for a certain time, but later on it behaves just like other ordinary nodes. Both Blackhole and Grayhole attacks disturb route discovery process and degrade network's performance [5].

In this paper, a mechanism to detect and remove these two types of attacks is proposed. In this proposed mechanism, an intermediate node receiving abnormal routing information from its neighbor node considers that neighbor node as a malicious node. The intermediate node appends the information about the malicious node in the route reply packet and every node receiving that reply packet then upgrades its routing table to mark the node as malicious node. When routing request is sent, a list of malicious node is appended to the packet and every node receiving the packet upgrades its routing table to mark the listed nodes as malicious. Thus, a node receiving fabricated routing information finds the malicious node either by identifying false routing information or by verifying its routing table; the node then tells other nodes not to consider the routing information received from the malicious node.

The remainder of paper is organized as follows. Section II describes related work. In Section III, proposed scheme is discussed for making MANET free from the Grayhole/Blackhole attack. Theoretical analysis of the proposed scheme is covered in Section IV. Finally conclusion and future directions are given in Section V.

II. RELATED WORK

Piyush et.al [6] proposed a solution where source and destination nodes carry out end-to-end checking to determine whether the data packets have reached the destination or not. If the checking fails then the backbone network initiates a

protocol for detecting malicious nodes. But, it works on assumption that any node in the network has more trusted nodes as neighbors than malicious nodes which may not be likely in many scenarios. If malicious nodes are more in numbers, this solution becomes vulnerable.

Chen et. al [7] presented a solution consisting of two related algorithms: key management algorithm based on gossip protocol and detection algorithm based on aggregate signatures. According to their solution, each node involved in a session must create a proof that it has received the message; when source node suspects some misbehavior, Checkup algorithm checks intermediate nodes and according to the facts returned by the Checkup algorithm, it traces the malicious node by Diagnosis algorithm. This solution may generate high traffic and computational cost of detection algorithm may be very high due to the basic limitations of gossip protocol and aggregate signatures.

A mechanism is proposed by Sukla et. al [8] in which before sending any block, source sends a prelude message to destination to make it aware about communication; neighbors monitor flow of traffic; after end of transmission, destination sends postlude message containing the number of packets received. If the data loss is out of acceptable range, the process of detecting and removing all malicious nodes is initiated by collecting response from monitoring nodes and the network. The mechanism has routing overhead increased due to additional routing packets.

For detecting packet forwarding misbehavior, Oscar et. al [9] proposed an algorithm that use the principle of flow conservation and accusation of nodes that are constantly misbehaving. Selecting correct threshold of misbehavior allows distinguishing well-behaved and misbehaved nodes. However, the average throughput cannot reach that of a network where there is no misbehaving node present because the algorithm requires definite time to gather the required data to identify and to accuse misbehaving nodes. Therefore, misbehaving nodes can drop packets before being accused and isolated from the network during the preliminary phase.

A trust-based approach is proposed by Arshad et. al [10] that uses passive acknowledgement as it is simplest; it uses promiscuous mode to observe the channel that allows a node to identify any transmitted packets irrelevant of the actual destination that they are intended for. Thus, a node can make sure that packets it has sent to the neighboring node for forwarding are indeed forwarded. Routing choices are made based on two parameters: trust and hop-count; therefore, the selected next hop gives the shortest trusted path. Though, monitoring overall traffic would have been a better choice instead of monitoring one node's request.

Ming-Yang et. al [11] proposed an intrusion detection system called Anti-Blackhole Mechanism (ABM) in which the suspicious value of a node is estimated according to the amount of abnormal difference between RREQs and RREPs transmitted from the node; all nodes perform ABM. With the requirement that intermediate nodes are prohibited to reply to RREQs, if an intermediate node is not the destination and never broadcasts RREQ for a specific route, but forward a RREP for the route, then its suspicious value will be increased in the nearby node's suspicious node table. When the suspicious value of a node goes beyond threshold, a Block message is broadcasted by the node to all other nodes in the network to isolate the suspicious node cooperatively. Though, the solution assumes that an authentication mechanism already exists in MANET.

An approach is discussed by Latha et. al [12] in which the requesting node waits for a specific time for replies from neighbors that include the next hop details. After the specific time, Collect Route Reply Table is verified to know whether there is any repeated next-hop-node or not. Existence of repeated next-hop-node in the reply paths indicates the truthful paths or limited chance of malicious paths. Though, the process of finding repeated next hop node increases overhead.

Payal et. al [13] suggested a protocol DPRAODV that finds a threshold value and compares that with difference of sequence number of reply packet and that of route table entry. If it is higher than the threshold value, the node sending reply is added to a list of blacklisted nodes. Also an ALARM packet containing blacklisted node is sent to its neighbors to inform that reply packets from the malicious node are to be discarded. The protocol has higher routing overhead due to addition of the ALARM packets.

An algorithm is proposed by Deng et. al [14] in which when a source node receives a route reply packet, it cross checks with the previous node on the route to the destination to verify that the node sending reply packet indeed has a route to the destination as well as to the intermediate node. If it does not have, the node that sent the reply packet is judged as malicious node. The mechanism, though, increases end-to-end delay and due to the addition of FurtherRequest and FurtherReply packets in the algorithm, routing overhead also gets increased.

III. PROPOSED APPROACH

To protect network-layer reactive protocols from Grayhole/Blackhole attacks, it is necessary to discover malicious nodes during route discovery process when they pass fabricated routing information to attract the source node to send data through itself. Our proposed approach does exactly the same.

In AODV protocol, when a node receives a route reply packet (RREP), it checks the sequence number value in routing table; if it is greater than the one in the RREP, the RREP packet is accepted; otherwise it is discarded [15]. Figure 1 shows the route discovery process in AODV in the presence of a malicious node M. Source node S broadcasts route request packet (RREQ); nodes within its communication range, A and C, receive the RREQ and re-broadcasts RREQ to their neighbors until a node having a valid route to the destination or destination D itself receives RREQ [16]. This node sends RREP to the source node on the reverse path of RREQ. The malicious node M sends RREP with higher, but fabricated, sequence number to the source; another RREP is sent by D having genuinely higher sequence number. As malicious node sends RREP with higher sequence number than the normal node, S chooses path through M to transfer data packets and therefore, malicious node can drop some or

all received packets which causes disruption in network operations.

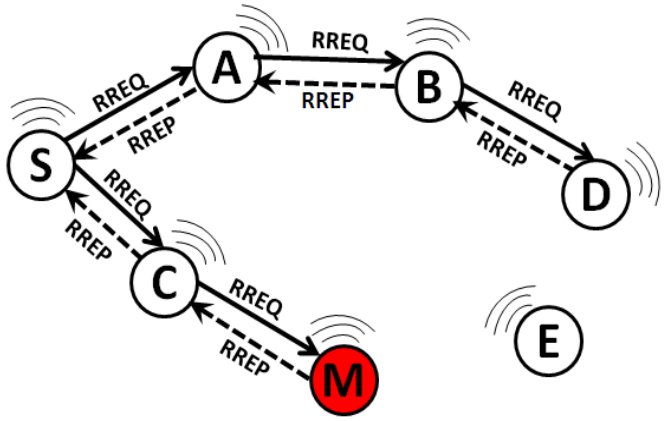

Figure 1. Route discovery process in AODV

In our proposed approach, an intermediate node dynamically calculates a PEAK value after every time interval [13] that uses three parameters for calculation: RREP sequence number, routing table sequence number and number of replies received during the time interval. The PEAK value is the maximum possible value of sequence number that any RREP can have in the current state. RREP received from malicious node is marked as DO_NOT_CONSIDER. Figure 2, Figure 3 and Figure 4 show the flowcharts of node receiving RREP, node sending RREQ and node receiving RREQ respectively.

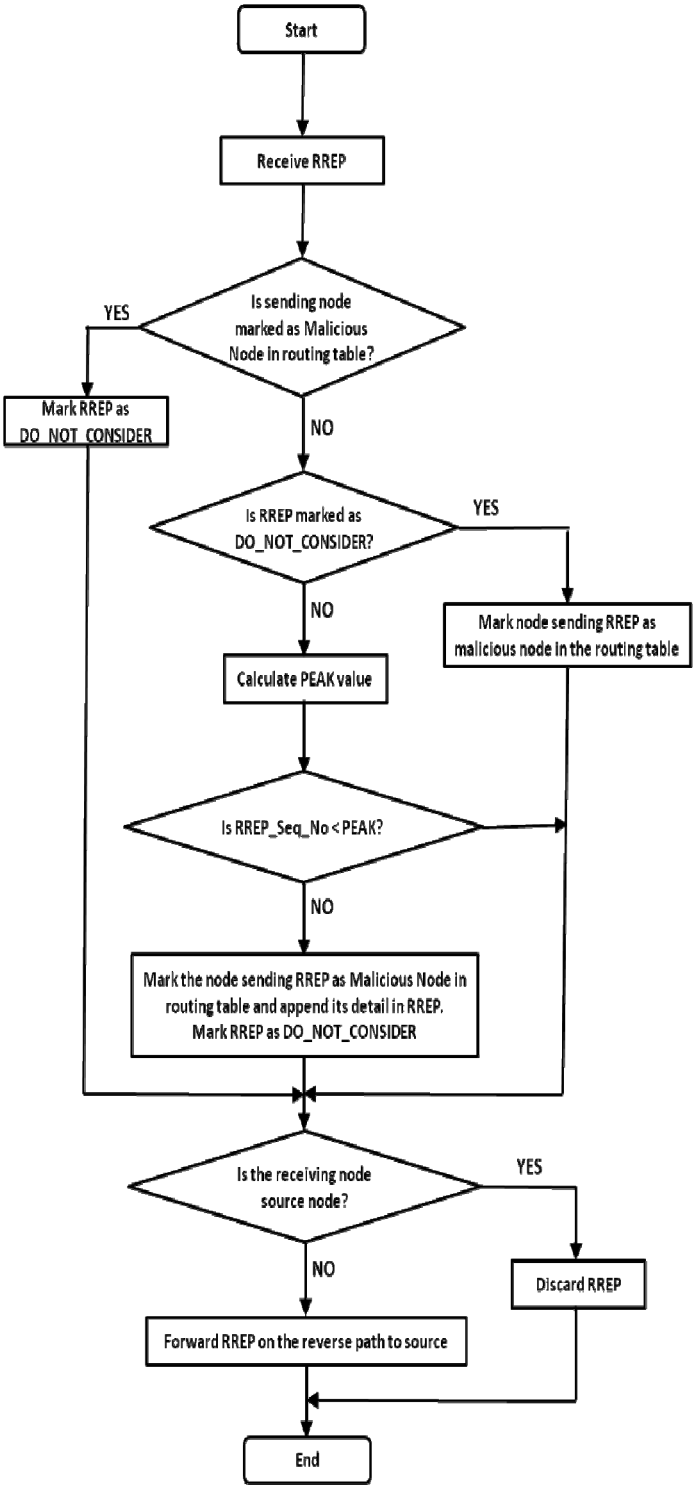

Figure 2. Flow chart for node receiving RREP

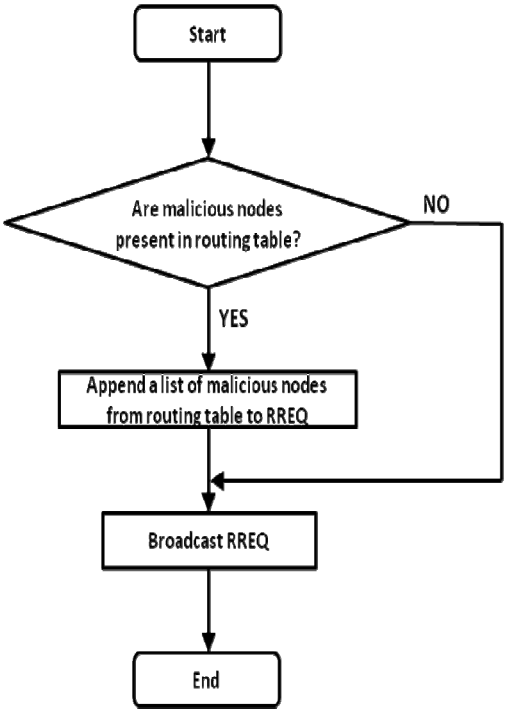

Figure 3. Flow chart for node sending RREQ

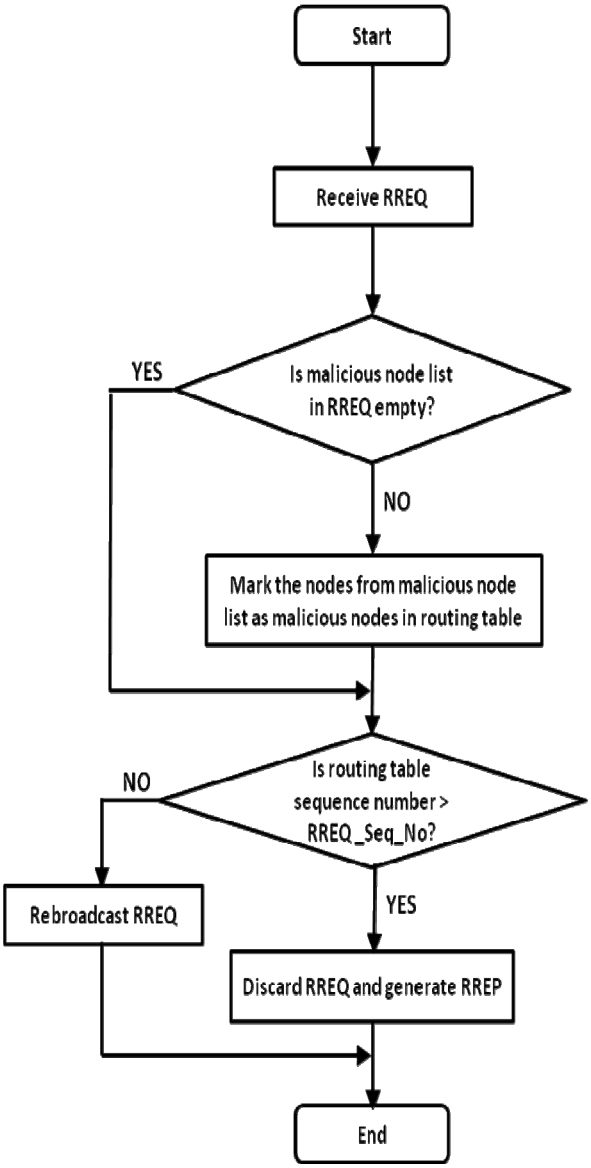

Figure 4. Flow chart for node receiving RREQ

With the proposed algorithm, when an intermediate node receives RREP having sequence number higher than the calculated PEAK value, it is marked as DO_NOT_CONSIDER; the node sending RREP is marked as malicious node in the routing table and RREP is then forwarded to the source node via reverse path. Meanwhile, each node receiving the forwarded RREP updates route entry for the malicious node. Source node sending RREQ also appends a list of malicious nodes to inform other nodes in the network about the existence of attackers. Thus, malicious nodes remain isolated from normal nodes.

As shown in Figure 5, S sends $RREQ_{ML}$ incorporating a list of malicious nodes detected till time to its neighbors A and C. Nodes A and C rebroadcasts the $RREQ_{ML}$ to their neighbors until nodes D and M receives it; both D and M sends RREP on the reverse path to S. When node C receives the abnormal RREP from M, it detects malicious behavior of M and marks the packet as DO_NOT_CONSIDER ($RREP_{DNC}$). C passes the

information about M on the reverse path to S and all intermediate nodes along with S update their routing table entry for M by marking it as a malicious node.

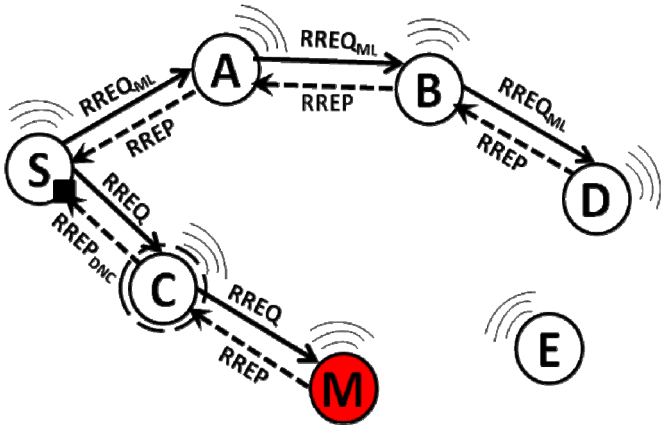

Figure 5. Route Discovery Process with proposed approach

IV. THEORETICAL ANALYSIS

The proposed algorithm detects and removes malicious nodes during the route discovery phase. Nodes receiving RREP verify the correctness of routing information; source node broadcasts a list of malicious nodes when sending RREQ. Nodes update route tables when they get any information of malicious nodes from received routing packets. As there is no extra control packets added in the proposed algorithm, there would be negligible difference in Routing Overhead which is the ratio of the number of routing related transmissions to the number of data related transmissions. Moreover, as the malicious nodes would be isolated, Packet Delivery Ratio (PDR) would be improved greatly; PDR is the ratio of number of received data packets to the number of sent data packets. If the node receiving RREP from a malicious node doesn't have the node marked as malicious in the routing table, the proposed algorithm adds a little computational overhead to that node as it has to calculate the PEAK value.

V. CONCLUSION AND FUTURE WORK

Security issues have been overlooked while designing routing protocols for ad-hoc networks. Through default AODV protocol, it is easier to breach the security of a MANET. AODV is susceptible to many DoS attacks including Grayhole and Blackhole attacks. In this paper, we investigated some of the existing solutions for these attacks and proposed a novel approach to counter these attacks that efficiently finds short and secure route to the destination. The theoretical analysis shows that our approach would greatly increase PDR with negligible difference in routing overhead. The algorithm is equally applicable to other reactive protocols.

As a part of our future work, we will implement our approach in ns-2and compare the results taking various metrics like PDR, Routing Overhead and End-to-End Delay by varying different network parameters.

REFERENCES

[1] Nadia Qasim, Fatin Said, and Hamid Aghvami, "Performance Evaluation of Mobile Ad Hoc Networking Protocols", World Congress on Engineering, 2008, pp. 219-229

[2] G.S. Mamatha and S.C. Sharma, "A Robust Approach to Detect and Prevent Network Layer Attacks in MANETS", International Journal of Computer Science and Security, vol. 4, issue 3, Aug 2010, pp. 275-284.

[3] Mohammad Al-Shurman, Seong-Moo Yoo and Seungjin Park, "Black Hole Attack in Mobile Ad Hoc Networks", ACMSE, April 2004, pp.96-97.

[4] Anu Bala, Munish Bansal and Jagpreet Singh, "Performance Analysis of MANET under Blackhole Attack", First International Conference on Networks & Communications, 2009, pp. 141-145.

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

[6] Piyush Agrawal, R. K. Ghosh and Sajal K. Das, "Cooperative Black and Gray Hole Attacks in Mobile Ad Hoc Networks", 2nd international conference on Ubiquitous information management and communication, 2008, pp.310-314.

[7] Chen Wei, Long Xiang, Bai Yuebin and Gao Xiaopeng,"A New Solution for Resisting Gray Hole Attack in Mobile Ad-Hoc Networks", Second International Conference on Communications and Networking in China, August 2007, pp. 366-370.

[8] Sukla Banerjee, "Detection/Removal of Cooperative Black and Gray Hole Attack in Mobile Ad-Hoc Networks", World Congress on Engineering and Computer Science , October 2008, pp. 337-342.

[9] Oscar F. Gonzalez, Godwin Ansa, Michael Howarth, and George Pavlou, "Detection and Accusation of Packet Forwarding Misbehavior in Mobile Ad-Hoc Networks ", Journal of Internet Engineering, vol. 2, no. 1, June 2008, pp. 181-192.

[10] Arshad Jhumka, Nathan Gri_ths, Anthony Dawson and Richard Myers, "An Outlook on the Impact of Trust Models on Routing in Mobile Ad Hoc Networks (MANETs)".

[11] Ming-Yang Su, "Prevention of Selective Black hole Attacks on Mobile Ad hoc Networks through Intrusion Detection Systems", Computer Communications, 2010.

[12] Latha Tamilselvan and Dr. V Sankaranarayanan, "Prevention of Blackhole Attack in MANET", The 2nd International Conference on Wireless Broadband and Ultra Wideband Communications, 2007, pp. 21-26.

[13] Payal N. Raj and Prashant B. Swadas,"DPRAODV: A dynamic learning system against black hole attack in AODV based Manet", International Journal of Computer Science Issues, Vol. 2, Issue 3, 2010, pp: 54-59.

[14] Hongmei Deng, Wei Li, and Dharma P. Agrawal, "Routing security in Wireless Ad-hoc Network",IEEE Communications Magazine, Issue 40, 2002, pp 70–75.

[15] Charles E. Perkins and Elizabeth M. Royer. "Ad-Hoc On- Demand Distance Vector Routing". In Proceedings of the Second IEEE Workshop on Mobile Computing Systems and Applications, Feb. 1999, pp. 90-100.

[16] Rutvij H. Jhaveri, Ashish D. Patel, Jatin D. Parmar and Bhavin I. Shah, "MANET Routing Protocols and Wormhole Attack against AODV", International Journal of Computer Science and Network Security, vol. 10 No. 4, April 2010, pp. 12-18.