# Review of Detection and Removal of Co-operative Black hole Attack in MANETs

**Nilay K Shah[1] Dr. Kalpesh Wandra[2]**

[1]M.E. Student [2]Principal

[1,2] Department Of Mechanical Engineering

[1,2]C.U.Shah College of Engineering and Technology, Wadhwancity, Gujarat, India

*Abstract*— A Mobile Ad-Hoc network in which nodes are mobile and it has dynamic topology which changes with mobility of nodes and also lack of centralization or lack of center controlling entity. These features came with undefined and unsecure boundaries makes challenging security. Black hole attack can in fact seriously compromise the performance of critical infrastructure of Mobile ad-hoc network. In this paper we proposed to detect and isolate multiple black hole attack during route discovery process and improve performance of Mobile Ad-Hoc network.

*Key words:* Black hole attack, MANET

## I. INTRODUCTION

A Mobile Ad hoc Network (MANET) is a system of wireless mobile nodes that dynamically self-organize in arbitrary and temporary network topologies. People and vehicles can thus be internetworked in areas without a preexisting communication infrastructure or when the use of such infrastructure requires wireless extension [3]. In the mobile ad hoc network, nodes can directly communicate with all the other nodes within their radio ranges; whereas nodes that not in the direct communication range use intermediate node(s) to communicate with each other. In these two situations, all the nodes that have participated in the communication.

Automatically form a wireless network, therefore this kind of wireless network can be viewed as mobile ad hoc network. The mobile ad hoc network has the following typical features [4]:

1) Unreliability of wireless links between nodes. Because of the limited energy supply for the wireless nodes and the mobility of the nodes, the wireless links between mobile nodes in the ad hoc network are not consistent for the communication participants.
2) Constantly changing topology. Due to the continuous motion of nodes, the topology of the mobile ad hoc network changes constantly: the nodes can continuously move into and out of the radio range of the other nodes in the ad hoc network, and the routing information will be changing all the time because of the movement of the nodes.
3) Lack of incorporation of security features in statically configured wireless routing protocol not meant for ad hoc environments. Because the topology of the ad hoc networks is changing constantly, it is necessary for each pair of adjacent nodes to incorporate in the routing issue so as to prevent some kind of potential attacks that try to make use of vulnerabilities in the statically configured routing protocol.

Because of the features listed above, the mobile ad hoc networks are more prone to suffer from the malicious behaviors than the traditional wired networks. Therefore, we need to pay more attention to the security issues in the mobile ad hoc networks.

A MANET (Mobile Ad hoc Network) is a collection of two or more devices equipped with wireless communications and networking capability. Such devices can communicate with another node that is immediately within their radio range or one that is outside their radio range. For the latter scenario, an intermediate node is used to relay or forward the packet from the source toward the destination. This kind of network is well suited for the mission critical applications such as- emergency relief, military operations, and terrorism response where no pre-deployed infrastructure exits for communication. Due to its intrinsic nature of lacking of any centralized access control, secure boundaries (mobile nodes are free to join and leave and move inside the network) and limited resources mobile ad-hoc networks are vulnerable to several different types of passive and active attacks[1], [2]. In this paper we tackle two types of routing attacks namely Black hole attack & Gray hole attack. In black hole attack a malicious node (called black hole) replies to every route request by falsely claiming that it has a fresh enough route to the destination. In this way all the traffic of the network are redirected to that malicious node which then dumps them all. A gray hole attack is a variation of black hole attack, where an adversary first behaves 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. Detection of gray hole attack is harder because nodes can drop packets partially not only due to its malicious nature but also due to overload, congestion or selfish nature.

## II. EXTENDED DATA ROUTING INFORMATION

The solution we are proposing tackles the black hole and gray hole attacks by maintaining an Extended Data Routing Information (EDRI) Table at each node in addition to the Routing Table of the AODV protocol. In [4] the DRI table is used for black hole detection at each node. It just has the through and from entries for other nodes of the network. But this is not sufficient in an environment where nodes might have a gray character. The DRI table in [4], although uses trust as a parameter but once trusted, a node is not doubted again. This is the loophole that might allow gray nodes to go

 

undetected. The EDRI table accommodates the gray behavior of nodes as well. Although, it gives subsequent chances to the nodes identified as black holes, it also keeps a record of the previous malicious instances of that node so that a better understanding of the node can be made and the node is given its next chance accordingly. A counter keeps track of how many times a node has been caught and the value of this counter is proportional to the time which has to pass before that node is given another chance. A node which is frequently being caught acting malicious is eventually not given a chance again.

Refresh packet, BHID Packet, Further request and further reply packets are also used in addition to the existing RREQ and RREP.

A refresh packet is sent by the source on the concerned path when it senses (with the help of NACK) that a malicious node might be active on that path. Each node that receives it has to refresh its DRI entries and delete the concerned path from its Routing Table.

A BHID packet has the identity of the malicious node that was identified using the algorithm. This packet is broadcast so that all the nodes can update their entries for the malicious node.

The further request and further reply packet are similar to the ones used in the [4] for black hole attacks but have some more info to accommodate the gray behavior. They are described in the following sections.

### *A. The EDRI Table*

An EDRI (Extended Data Routing Information) Table is maintained at each node. The table is gradually updated as nodes interact with one another. Suppose the Table I is the EDRI table maintained at Node 1.

#### *1) FROM*

This entry shows if node in question i.e. node 1 here has routed data packets that originated at the particular node id. A 0 stands for false i.e. it has not routed data packets. A 1 on the other hand means that data packets have been routed.

| Node_id | From | Through | Counter | BH | Timer |
|---|---|---|---|---|---|
| 4 | 0 | 1 | 1 | 0 | 0 |
| 5 | 1 | 1 | 0 | 0 | 0 |
| 8 | 0 | 0 | 2 | 0 | 0 |
| 10 | 0 | 0 | 8 | 1 | $2^8$ |

Table. 1: EDRI Table at node 1

#### *2) THROUGH*

This field is similar to the previous field i.e. it has a value 1 if the node id has successfully routed data packets that were sent by node 1.Note that a 0 value in from & through columns does not mean that the node is malicious or it cannot be used, it just means that it cannot be trusted to be an honest node. There just has not been an interaction.

#### *3) CTR*

CTR keeps a count of the number of times the node behaved maliciously.

#### *4) BH*

This entry is 1 if the node id has been identified to be malicious in its latest interaction else it is 0. The BHID packet is used to update this field. Example, Node 10 is being treated as a black hole at this point.

#### *5) TIMER*

This field has the duration for which the node would be considered malicious i.e. it would not be considered for routing data. The value is determined using the value of the CTR field. As an example, the current scenario is using an exponential function to determine the value of this field from CTR.

Another important point here is that the EDRI values should be consistent i.e. if node A has routed through node B, node A would have a 1 in through entry for node B and Node B would have a 1 in the from entry for node A. The from and through entries might therefore seem redundant at first but the inconsistency in these values is what is instrumental in identifying the black hole node. How it is done is explained in the following sections.

## III. MODIFIED RELIABLE AODV

As an attempt to further improve performance of MANET, we further modify the functionality of node receiving RREP in R-AODV. Fig. 1 [7] compares the route discovery processes of R-AODV and Modified R-AODV (MR-AODV) in presence of a malicious node. As shown in Fig. 1(a) [7], when a malicious node is detected by an intermediate node after receiving RREP, R-AODV marks the RREP as DO_NOT_CONSIDER and marks the node sending RREP as MALICIOUS_NODE in the routing table; the RREP is then forwarded on the reverse path to the source which updates routing tables of all the nodes on the reverse path with malicious node entry; a route towards destination is chosen by selecting unmarked RREPs.

On the other hand, in MR-AODV, when a node detects a malicious node, it updates the routing table with malicious node entry and discards the RREP as shown in Fig. 1(b); it is neither forwarded on the reverse path nor requires a DO_NOT_CONSIDER flag; thus, all RREPs reaching to the source node will be sent by genuine nodes only; the RREP indicating shortest fresher path will be chosen for data transmission by the source node.

Thus, MR-AODV attempts to reduce routing overhead by not forwarding RREP after detection of misbehavior. In the following subsection we represent design of MR-AODV in form of flow-charts based on the designs discussed in [2], [6] and [7].

### *A. Design of Algorithm*

We present the functionalities of node sending RREQ, node receiving RREQ and node receiving RREP in form of flow-charts as follows:

#### *1) Node broadcasting RREQ*

Fig. 2 [2] shows the functionality of node broadcasting RREQ.

#### *2) Node receiving RREQ*

Fig. 3 [2] represents the functionality of node receiving the broadcasted RREQ.

#### *3) Node receiving RREP*

Fig. 4 [2][6][7]depicts the functionality of node receiving RREP.

 

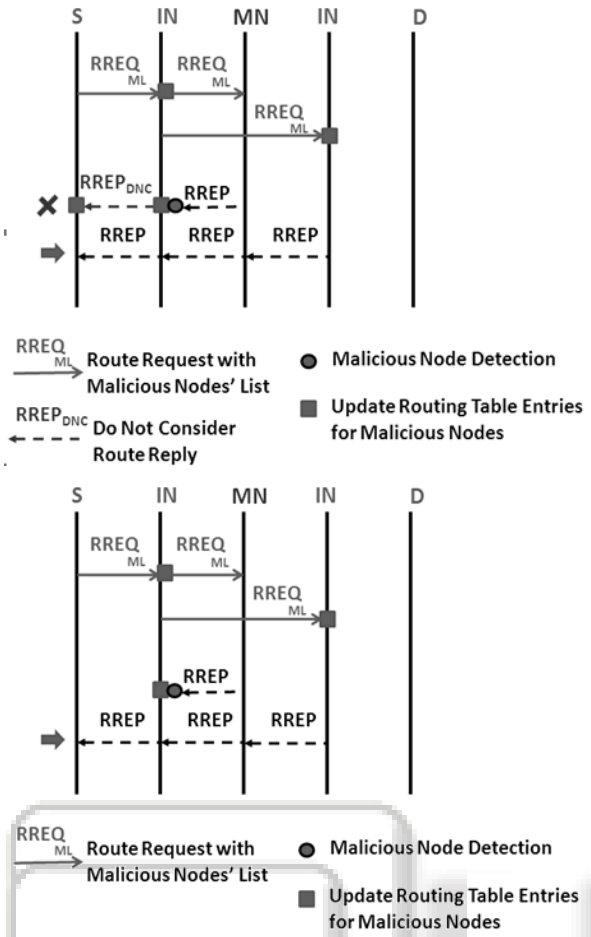


Fig. 1: Comparison of route discovery processes of R-AODV and MR-AODV under attack

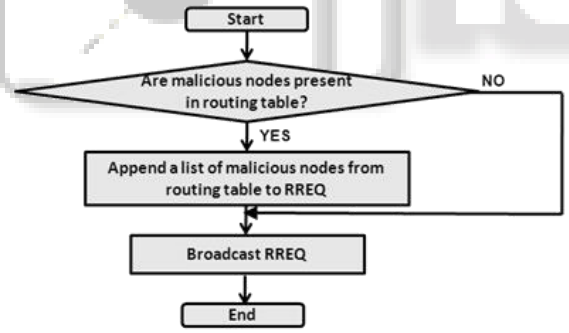


Fig. 2: Flow chart for node broadcasting RREQ

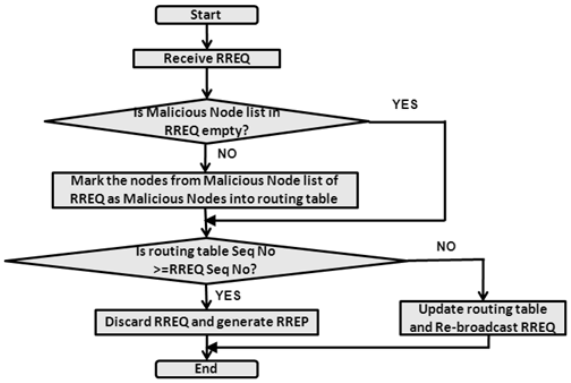


Fig. 3: Flow chart for node receiving RREQ

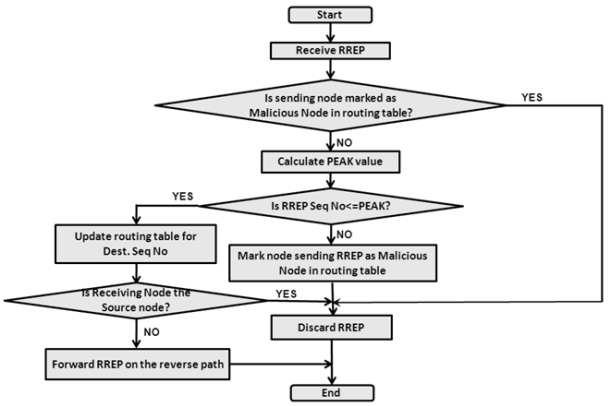


Fig. 4: Flow Chart for node receiving RREP

## IV. CONCLUSION

Default ad-hoc routing protocols are prone to various DoS attacks due to ignorance of security aspect during their designs. Black hole and Gray hole attacks disrupt normal network. Functionality by sending bogus routing information during route discovery and construction phase. In this paper, we investigated further existing approaches to tackle Black hole and Gray hole attacks and discussed our previous research work. We propose a modified protocol viz. MR- AODV based on our previous finding viz. R-AODV that eliminates limitations of existing mechanisms. MR-AODV isolates Black hole and Gray hole nodes during route discovery phase as R-AODV and sets up a secure route for data transmission. It attempts to further reduce normalized routing overhead by decreasing number of forwarded reply packets sent by adversaries. Simulation results presented in form of graphs prove that MR-AODV is a reliable solution which gives significant improvement in PDR with acceptable average end-to-end delay and normalized routing overhead under various network parameters and traffic conditions.

## REFRENCES

[1] Jia Uddin and Md. Rabiul Zasad, "Study and Performance Comparison of MANET Routing Protocols: TORA, LDR and ZRP", A Master's Article in Electrical Engineering, School of Engineering, Blekinge Institute of Technology, Sweden, May 2010.

[2] Rutvij H. Jhaveri, Sankita J. Patel and Devesh C. Jinwala, "A Novel Approach for Grayhole and Black hole Attacks in Mobile Ad-hoc Networks", In Proc. of International Conference on Advanced Computing & Communication Technologies: Conference Publishing Services (CPS), January 2012, pp.556-560.

[3] Akanksha Saini and Harish Kumar, "Comparison between Various Black Hole Detection Techniques in MANET", In Proc. of National Conference on Computational Instrumentation, March 2010, pp. 157-161.

[4] Rutvij H. Jhaveri, Sankita J. Patel and Devesh C. Jinwala, "DoS Attacks in Mobile Ad- hoc Networks: A Survey", In Proc. of International Conference on Advanced Computing & Communication Technologies: Conference Publishing Services (CPS), January 2012, pp.535-541.

 

[5] Bala A., Bansal M. and Singh J., "Performance Analysis of MANET under Black hole Attack", In Proc. of First International Conference on Networks &Communications, December 2009, pp. 141–145.
[6] Rutvij H. Jhaveri, Sankita J. Patel and Devesh C. Jinwala, "A Novel Solution for Grayhole Attack in AODV Based MANETs", In Proc. of Third International Conference on Advances in Communication, Network and Computing: Springer, February 2012. pp. 60-67.
[7] Rutvij H. Jhaveri, Sankita J. Patel, Devesh C. Jinwala, "Improving Route Discovery for AODV to Prevent Black hole and Grayhole Attacks in MANETs", INFOCOMP Journal of Computer Science. March 2012, Vol. 11 No. 1, pp. 1-12.
[8] Ira Nath and Dr. Rituparna Chaki, "BHAPSC: A New Black Hole Attack Prevention System in Clustered MANET", International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 2 Issue 8, August 2012, pp. 113-121.
[9] Moumita Deb, "A Cooperative Black hole Node Detection Mechanism for ADHOC Networks", In Proc. of the World Congress on Engineering and Computer Science 2008, October 2008.
[10] Surana K.A., Rathi S.B. Thosar T.P. and Snehal Mehatre, "Securing Black Hole Attack in Routing Protocol AODV in MANET with Watchdog Mechanisms", World Research Journal of Computer Architecture, Vol. 1 Issue 1, 2012, pp. 19-23.
[11] Jain, S., Jain, M., and Kandwal H., "Advanced Algorithm for Detection and Prevention of Cooperative Black and Gray hole Attacks in Mobile Ad hoc Networks", International Journal of Computer Applications, Vol. 1 No. 7, pp. 37-42.
[12] Kevin Fall, Kannan Varadhan: The ns Manual, http://www.isi.edu/nsnam/ns/doc/
[13] F. J. Ros and P. M. Ruiz, "Implementing a New MANET Unicast Routing Protocol in NS2", http://masimum.dif.um.es/nsrt-howto/pdf/nsrt-howto.pdf,December2004.

 