International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Cooperative Gray Hole Attack Detection and Prevention Techniques in MANET: Review

Shani Makwana[1], Krunal Vaghela[2]

[1]PG Scholar, Computer Engineering, RK University, Rajkot, Gujarat, India

[2]Dy. Director, School of Computer Science, RK University, Rajkot, Gujarat, India

Abstract: ***MANET (Mobile Ad Hoc Network) is a type of ad hoc network that can change locations and configure itself, because of moving of nodes. As MANETs are mobile in nature, they use wireless connections to connect various networks without infrastructure or any centralized administration. Open medium, dynamic topology, distributed cooperation are the characteristics of MANET and hence ad hoc networks are open to different types of security attacks. This paper represents a review of different techniques of gray hole attack detection and prevention on AODV routing protocol. All the techniques are having some advantages and disadvantages. Among all of these techniques, the credit based technique gives better performance in terms of end to end delay, throughput and packet delivery ratio. The results can be improved in different cases under various scenarios like pause time, number of nodes and varying speed of nodes.***

Keywords: MANET, AODV Routing Protocol, Gray Hole Attack

1. Introduction

MANETs [1] form a temporary network of mobile nodes, which is infrastructure less. In this network, intermediate nodes cooperate and act as a router and send messages from one node to another. It is quite useful in situations where we have lack of fixed network infrastructure, such as an emergency situations or rescue operation, medical assistance, disaster relief services, mine site operations, and military mobile network in battlefields. [1] MANETs are having problems of dynamically changing network topologies, no infrastructural support, and limited bandwidth. For researcher it has been quite an interesting research area in designing a routing protocol discovering the best possible route in a dynamic environment of MANET's.[1] Because of not having any fixed infrastructure and dynamically changing network topology, MANETs are exposed to different threats. This leads to different types of security attacks. These are Black hole Attack, Flooding Attack, Gray Hole Attack, Worm Hole Attack, Sinkhole Attack and many others.

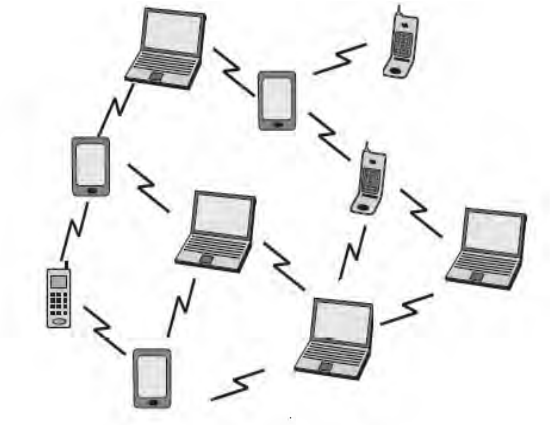

Figure 1: Mobile Ad Hoc Network [2]

A. Characteristics of MANET

1) *Dynamic Topologies:*
The nodes of the network are keeps on moving with different speeds, which results in the variations in the structure of the network.
2) *Energy-constrained Operation:*
The devices in the modern electronic world completely rely on batteries. The design of the network is to be improved to conserve the energy consumed by the mobile nodes.
3) *Limited Bandwidth:*
The bandwidth of the wireless network is very narrow and the networks are to be optimized to perform with the maximum efficiency with in the limited bandwidth.
4) *Security threats:*
When compared to the wired communication with wireless, the wireless communication is more affected for security. The security of the MANET is to be improved so that the information transferred is secured. [3]

2. AODV Routing Protocol

Ad hoc on-demand distance vector(AODV) [4] routing protocol uses an on demand approach for searching routes, that route is established only when it is required by source node for transmission of data packets. It applies a destination sequence numbers to identify the latest recent path. In an AODV, the source node broadcasts the RREQ message in the network when the route is not available for the destination. [4] A node refresh its path information only if the Destination Sequence Number of the current packet received, is greater than the last DesSeqNum stored at the node. When any of intermediate nodes receives a Route Request, it either forwards or provides a Route Reply, if it has a valid route to the destination. [4] All the intermediate nodes having valid routes to the destination or the destination node itself, only that much nodes are allowed to send RREP packets to the source back. When a node receives a RREP packet, information about the previous node from which the packet is received is also reserved in order to forward the data packet to this next node as the next hop against the destination. [4]

AODV cannot re-establish a broken path. But, whenever link breaks, it is determined through acknowledgements. Hence, source node is come to know about the path break and it reconstructs route to the destination if required by higher layers. If path break is detected at an intermediate node, the node warns the end nodes by sending a voluntary RREP with the hop count set as ∞. [4]

3. Gray Hole Attack

Gray hole is one of the attacks initiate in ad hoc network. This acts as a slow toxic in the network. Hence, we cannot suppose how much data can be lost. In gray hole Attack [5], a malicious node trashes to lead certain packets and just drops them. The attacker selectively drops the packets originating from a single IP address or a range of IP addresses and forwards the remaining packets. Grayhole nodes in MANETs are very effective. Every node preserves a routing table, which keeps the next hop node information for a route a packet to destination node. When source node wants to route a packet to the destination node, it uses a particular route if such a route is available in its routing table. [5] If not then nodes start a route discovery process by broadcasting Route Request (RREQ) message to its neighboring nodes. By getting the RREQ message, the intermediate node finds the most recent path in their routing tables in a reverse route to the source node. A RREP is sent back in reverse direction of the source node, after the RREQ query reaches either the destination node itself or any other intermediate node that has a fresh route to destination. Now here, we define the gray hole attack [6] on MANET'S. The gray hole attack has two major phases.

In first phase, a malicious node accomplishes the AODV protocol to declare itself as having a valid route to destination node, with the intension of including or confusing the packets, even though route is fake. [6] In second phase, the malicious nodes drop the irregular packets with a certain vision. The process of finding gray hole is very challenging task. In some cases grayhole attack is also called as node misbehaving attack. The black hole attack differs from the grayhole attack is that the affected nodes either drop packets selectively. [6]

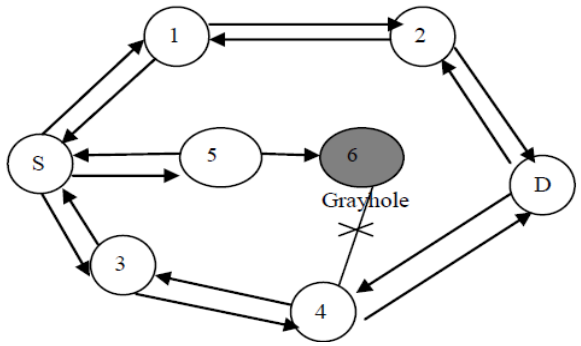

Figure 2: Gray Hole Attack [7]

4. Literature Survey

A. Technique to detect malicious node using DRI table:
In [8] the security procedure is invoked by a node when it founds a suspicious node by examining its DRI table. The node that initiates the suspected node recognition procedure is known as the Initiator Node (IN). The IN first chooses a Cooperative Node (CN) in its region, based on its DRI records and broadcasts a RREQ message to only its 1-hop neighbors requesting for a route. [8] In reply to this RREQ message the IN will receive a number of RREP messages from its adjacent nodes. It will definitely receive a RREP message from the Suspected Node (SN) which, the latter is really a gray hole. As RREP is received from the SN, the IN sends a query packet to the CN through the SN. After the time to live value of the query packet is over, the IN checks the CN whether it has received the query packet or not. If the reply to this query is positive, then the IN modifies its DRI table. [8] However, if the query packet is found to be not reached to the CN, the IN increases its level of suspicion about the SN and starts the suspicious node recognition procedure.

B. Attack detection using higher sequence number and PEAK value:
In proposed AODV protocol [9], when node receives a route reply packet (RREP), it checks the sequence number in routing table. If the sequence number is greater than the one in the RREP, the RREP packet is accepted otherwise it is discarded. The route discovery process in this is done in the presence of a malicious node. [9] Source node broadcasts route request packet (RREQ) to the nodes within its neighborhood area or sort communication range. When neighbor node receive the RREQ and rebroadcasts RREQ to their neighbors until a node having a valid route to the destination or destination itself receives RREQ packets. This node sends RREP to the source node on the reverse path on which RREQ sent. The malicious node sends RREP with higher but fabricated sequence number to the source. And another RREP is sent by destination node, having actually higher sequence number. [9] As malicious node sends RREP with higher sequence number than the usual node, source node selects path through malicious node to transfer data packets. And malicious node can drop some or all received packets which leads network to the performance degradation. Also in this the intermediate node dynamically calculates a PEAK value after fixed time interval. This uses three parameters for calculation: RREP sequence Number, Number of replies Received during the time interval and Routing table sequence number. [9] The PEAK value is the highest possible value of sequence number that any RREP can have in its current state. RREP received from malicious node is marked as DO_NOT_CONSIDER. Now, when an intermediate node receives RREP having higher sequence number than the calculated PEAK value, it is marked as DO_NOT_CONSIDER. [9] The node, which is sending RREP, is marked as malicious node in the routing table. RREP is then forwarded to the source node via reverse path to the source. In the meantime, each node receives the forwarded RREP updates route entry for the malicious node. Source node sends RREQ that append a list of malicious nodes to inform other nodes in the network about the presence of attacker. Hence, malicious nodes remain remote from other normal nodes. [9]

C. Gray hole attack detection using credit based technique:
In this proposed approach [10], the AODV protocol is a little modified and an new algorithm is known as Credit Based

AODV (CBAODV). In which, firstly each and every node assigns a permanent value for its every adjacent node as the neighbor credit value. This credit value is increases by the protocol when it receives a route request packet (RREQ) and decreases when it receives the route reply (RREP) packet. When a node finds negative credit value for one of its neighbors, then it detected as the gray hole attacker. [10] This also removes all current established paths from its routing table which is going through that node. Each node assigns a credit value that we are sending the route request and subtracting the credit value when we got a reply from them. This algorithm is capable to detect cooperative grayhole nodes. [10]

D. Attack detection using second shortest route to destination and message digest:

In this proposed solution [1] we have changed our scheme and it contains three parts. In the first part we want to make slight changes in AODV. In this method, we have to use second shortest path for data packets transmission instead of using first path for transmission. Source node transmits the route request packet (RREQ) to the destination, which broadcasts in the whole network. We assume that this message is reached to the destination through many different paths. The first path is the shortest path to the destination due to very less number of nodes. [1] There might be chances to present some malicious node in the route. Thus, malicious node can simply become part of the route, through which data can be sent. We desire that the receiver node have to wait for receiving the second route request and sends the route reply (RREP) message on this route back again. The source node can then send data packets successfully on this route to the destination node just because the malicious node will not be able to know that through which route the data will come. It also may happen that malicious node can be a part of second shortest path. [1] For this, we desire to apply a hash function on message that has to be sent to get a unique message digest (MD). Source node sends the MD with the first data packets to the receiver and receiver node stores this MD with itself. When the receiver gets all the data packets, it applies a hash function on the message to get a message digest. [1] Then it compares this message digest with the stored one message digest. If both the messages are equal, that means the message has been received successfully and there is no attacking node in the route. But if they are not equal, it means some data packets have been dropped in the data transmission and there is presence of malicious node in the network. After detecting the malicious node, the receiver broadcasts Data Packets Received Error (DPRE) message to the source node to re-establishes a new route to the destination. [1]

E. Detection and Removing of black/gray hole attacks using source node, destination node and neighbor node:

Detection process for gray hole /black hole attack by source node: [11]

1. Dividing data packets into *k* equal parts.
2. Sending a message to destination containing number of messages.
3. Broadcasting messages to all neighbors of route.
4. After ensuring that destination node knows count of messages, source begins sending of data.
5. Setting up a timer until getting number of data packets that destination receives.
6. If number of announced data packets from destination is less than a limit, initiates removing process of black/gray hole attack.
7. Also if after terminating of timer, did not get any message from destination, starts removing process of black/gray hole attack.

Detection process for black/gray hole attack by destination node: [11]

After knowing the number of data packets that are sent from source node, setting a timer to zero and starts counting data packets. After a timeout, returns data packet numbers to source node. Detection process for black/gray hole attack by neighborhood nodes: [11] By monitoring message from source node, each node starts a counter for counting number of data packets of its neighbors. Remove process for black/gray hole attack by source node: [11]

1. Source node gets vote of one node's neighbors about the maliciousness.
2. According to the votes of neighbors, starts counter for malicious node in Find Malicious table.
3. If votes of neighbors about maliciousness exceeds from a limit, source enters that node in Gray/Black hole table and finds a new route to destination. Also announces to the network that the node is a malicious node.

Remove process for black/gray hole attack by neighbor nodes: [11]

When they get monitoring message, they start counting numbers of packets that malicious node sends. If number of passed messages is less than a limit then it inform about it to source node.

F. Detection using Local collaboration and Information cross-validation:

SCAN [12] uses two ideas to defend AODV in MANET: Local collaboration and Information cross-validation.

- In Local collaboration, nodes monitor each other and also maintain routing tables of each other. Each node uses a token that validate itself to the network. If one node is suspected to be malicious, other nodes invalidate its token and alert token revocation to all nodes in network and they insert that node in their token revocation list. So, the malicious node does not have any access to the network.
- In Information cross-validation, each node checks routing packets came from its neighbours. Each node knows every neighbour's routing tables, which can cross-check the overheard transmissions of them.

G. Detection of gray hole attack using trustful nodes:

In [13] there are some extra nodes-strong nodes, which help source and destination to find black and gray hole attacks. These strong nodes are assumed to be trustful and also capable of tuning its antenna to large ranges and short ranges. Each normal node is inside the range of one of these strong nodes. By using the strong nodes, source and destination starts to check if the data packets have reached the destination or not. [13] If any changes found in number of messages sent from source and received at destination, strong nodes ask the nodes in their areas about the monitoring

results of one node's behaviour. If the checking results show misbehaviour according to the votes, then the network runs a protocol which can detect black or gray hole attack. At last announces malicious node to the network by broadcasting messages. [13]

5. Discussion

Table 1: Advantages and disadvantages

Techniques	Advantages	Disadvantages
Detection using DRI table	Analyzed the impact of gray hole attack with terms PDR and e2e value.	In proposed algorithm, some extra fields are added so more memory required.
Detection using Higher sequence number and PEAK value	As the malicious node isolated, PDR would be improved. No extra control packets added so, negligible Change in Routing Overhead.	There is no limit for detection of malicious node that increases mistakes.
Detection using Credit based technique	This paper presents good performance in terms of better throughput and minimum packet loss.	It consumes more energy due to credit assigning to each node.
Detection using Second shortest route to destination and Message digest	This decrease the probability of malicious node present in second route. Message digest provides data integrity.	Energy consumption is more because of message digest.
Detection using source node, destination node, neighbor node	Decreases number of mistakes in identifying black/gray hole attack.	Detection speed for malicious nodes is low. Consumes a lot of energy for monitoring.
Detection using local collaboration and Information cross-validation	Each node uses a token which authenticates the node to the whole network.	Mistakes in finding malicious nodes will be increased. Not any neighbor node presents, then this method does not work.
Detection using trustful nodes	Strong nodes decrease the number of monitoring of neighbours.	Assumes that strong nodes are trustable. There is no limit for detection of maliciousness of one node that increases mistakes.

6. Conclusions

Mobile Ad-hoc Network is the most challenging field in the wireless network. The challenge that the MANETs are facing most is MANET security. In this paper, we have seen that, how gray hole attack happened in network. The gray hole attack is require to detect and prevent, acts as a normal node in the network, which is hard to find. Here, we have reviewed different techniques to detect and eliminate the gray hole attack on AODV routing protocol. The purpose of reviewed different techniques in this paper is, to find the efficient technique to detect gray hole attack and how it can be eliminated to improve network security and performance of the network.

References

[1] Hizbullah Khattak, Nizamuddin, "A Hybrid Approach for Preventing Black and Gray Hole Attacks in MANET", *Digital Information Management (ICDIM) Eighth International Conference*, pp. 55-57, IEEE September 2013.
[2] M. Kumar, R. Mishra, "An Overview Of MANET: History, Challenges and Applications", *IJCSE*, Vol. 3 No. 1, pp. 121-125, Feb-Mar 2012.
[3] Characteristics of MANET(online) available: http://techupdates.in/what-is-manet-characteristics-and-applications-of-manet-in-communication/
[4] C. Siva Ram Murthy, B. S. Manoj, *Ad Hoc Wireless Networks: Architectures and Protocols*, Person Education, ISBN 978-81-317-0688-6, 2004.
[5] K. Vishnu, A. J. Paul, "Detection and removal of cooperative black/gray hole attack in mobile *adhoc* networks", *IJCA(0975-8887)*, Vol. 1 No. 22, pp. 38-42, 2010
[6] Sukla Banerjee, "Detection/Removal of Coperative Black and Gray Hole Attack in Mobile Ad-hoc Networks", *Proceedings of the World Congress on Engineering and Computer Science 2008*, October 22-24, 2008.
[7] Harsh Pratap Singh, Virendra Pal Singh, Rashmi Singh, "Cooperative Blackhole/ Grayhole Attack Detection and Prevention in Mobile Ad hoc Network: A Review", *International Journal of Computer Applications (0975 – 8887)*, Volume 64– No.3, pp. 16-22, February 2013.
[8] Onkar V. Chandure, V. T. Gaikwad, "Detection & Prevention of Gray Hole Attack in Mobile Ad-Hoc Network using AODV Routing Protocol", *International Journal of Computer Applications(0975-8887)*, Volume 41- No.5, pp. 27-32, March 2012.
[9] R. H. Jhaveri, S. J. Patel, D. C. Jinwala, "A novel approach for Grayhole and Blackhole attacks in Mobile Ad-hoc Networks", *Second International Conference on Advanced Computing & Communication Technologies*, IEEE, pp. 556-560, 2012.
[10] Deepali A. Lokare, A.M Kanthe, Dina Simunic, "Cooperative Gray Hole Attack Discovery and Elimination using Credit based Technique in MANET", *International Journal of Computer Applications (0975-8887)*, Volume 88-No.15, pp. 13-22, February 2014.
[11] S. Jain, M. Jain, H. Kandwal, "Advanced algorithm for detection and prevention of cooperative Black and Gray hole attacks in mobile ad hoc networks", *IJCA (0975-8887)*, Vol. 1-No. 7, pp. 37-42, 2010.
[12] Yang, H., Shu, J., Meng, X., and Lu, S., "SCAN: Self-organized network-layer security in mobile ad hoc networks", *IEEE journal*, Vol. 24-No. 2, pp. 261-273, Feb-2006.
[13] P. Agrawal, R. K. Ghosh and S. K. Das, "Cooperative black and gray hole attacks in mobile ad hoc networks", *In Proceedings of the 2nd International Conference on Ubiquitous Information Management and Communication*,pp.-310-314,January-2008.