ISSN:2249-5789

A Survey Paper On Detection Of Gray-Hole Attack in MANET

Nirali Modi[1], Vinit Kumar Gupta[2], Indr jeet Rajput[3]
[1] Hasmukh Goswami College of Engineering, Ahmedabad, India
modinirali7@gmail.com
[2] Hasmukh Goswami College of Engineering, Ahmedabad, India
guptasvnit@gmail.com
[3] Hasmukh Goswami College of Engineering, Ahmedabad, India
Indr.rajput@gmail.com

Abstract-MANET is a wireless ad hoc network, decentralized network and autonomous system. Mobile ad hoc network is created by mobile nodes. To forward the packet, each node in MANET acts as router. That is free to moving in and out in the network. There are some constraints like limited resources, self – configuration ability, power consumption ratio and security. Among them security is the most challenging job in MANET to maintain the networks performance. There are different types of attacks detected in MANET. Denial–Of-Service (DOS) attacks are detected on network layer which are namely as gray hole attack, black hole attack and worm hole attack. We have surveyed research papers based on detection of gray hole attack in MANET. This survey paper analyze the gray hole attack detection technique on AODV routing protocol.

Keywords—MANET, gray hole, AODV, RREQ, RREP

I. INTRODUCTION

Most important concern for network is security in mobile ad hoc network. It is highly adaptable and deployable network. It is a self- configuring infrastructure less network of mobile devices connected by wireless. Radio communication is used by mobile nodes. Basically there are two types of attacks.

Active attack:

Active attack can be external or internal. They can disturb the network's task by alarming the false message or modifying information. Internal attacks are attacker within the network and external network are outside the network by carried out nodes that do not belongs to the network e.g. modification, jamming and message reply.

Passive attack:

Passive attacks are difficult to detect and does not disturb the network's performance or operation e.g. traffic analysis, traffic monitoring.

Gray hole attack detects on the network layer. It can be act as slow poison. It is the variation of black hole attack. In gray hole attack malicious node either drop packets selectively or

Refuse to forward packets and drop them (e.g. dropping 50% of packet or dropping with some probability or forward all TCP packets while dropping all UDP packets). Malicious node some

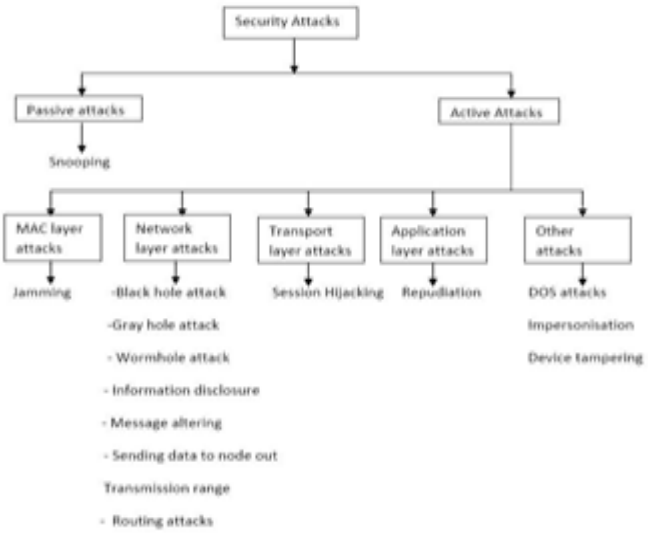

Fig 1: Security Attacks for different layers. [3]

Time acts as normal node after dropping packets. Due to these constraints it is difficult to maintain network's performance good. [2,3] and very hard to find out this kind of attack. It has two phases. In First phase the malicious node advertises AODV routing protocol as a fresh and valid route to reach the destination node. In second phase node drop the packet with

50% of probability and switch from malicious to normal mode [4]. Gray hole attack is an active attack. In gray hole attack some packets are dropped during the request send by source node. After that source gets some replies from intermediate node and assigns the route path. fig 2. Shows the process of gray hole attack in which one node is malicious node and it will drop the packet. Then after malicious node behave as normally node to others and claims that it does not dropped the packet. It is also known as misbehaving attack because of its misbehavior in forward the packets. Due to its misbehavior it is very difficult for network to figure out such kind of attack. [2].

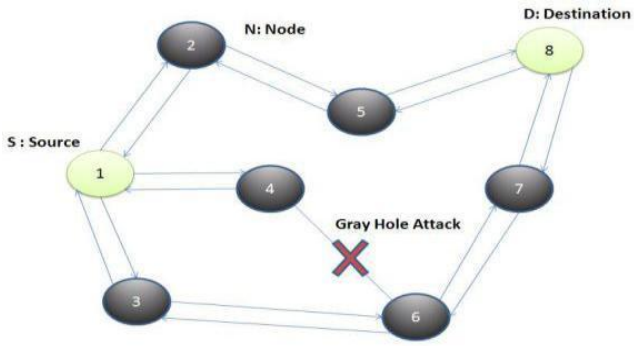

Fig.2 Gray hole attack [4]

II. AODV ROUTING PROTOCOL

Ad-hoc-on-demand distance vector (AODV) routing is a routing protocol that is used in wireless ad hoc network and mobile ad hoc network. it is developed in Nokia research center of networks. It is an on –demand routing protocol so route is established only on demand based destination. It is used in multicast and unicast routing. To ensures the valid route or freshness of routes sequence numbers are used by AODV protocol. It is loop-free and integrates a large number of nodes. For route maintenance three types of control message are used by AODV.

RREQ: Whenever a node requires a route it transmit route request message. RREQ carries a TTL value that shows the hops of the messages should be forwarded; the RREQ contains the source address, broadcast ID, source sequence number, destination address, destination sequence number, hop count.

RREP: If the receiver is either node using requested address or it has a valid route to the destination address then route reply message is transmitted back to the origin node.

RRER: To check the link status of next hop in active routing process nodes monitors the link status. There are some advantages like in this protocol to find the latest route to the destination sequence number are used or applied and it have routes established on demand.

III. LITERATURE SURVEY ON GRAY HOLE ATTACK DETECTION SCHEME

A. A Novel Gray hole attack detection scheme for mobile ad hoc networks [6]

In this paper author propose three algorithms to detect malicious node.

1). Creating proof algorithm in this algorithm each node involved in a session should create a proof based on aggregate signature algorithm to demonstrate it has received.

2). the check up algorithm which defines the source node suspects that the packet dropping attack has happened.

3). the diagnosis algorithm defines evidences returned b the checkup algorithm; the source node could trace the malicious node.

B. Detection/Removal of cooperative black and gray hole attack in mobile ad hoc networks [7].

The author proposes a technique to find the chain of cooperating malicious node which drops a fraction of packet. Instead of sending a total data traffic at a time divide the total traffic into some small sized blocks. So that malicious node can be detected and removed in between the transmission of two such blocks by ensuring an end-to-end checking. Source node sends a prelude message to the destination node before start of sending any block to alert it about incoming data block. Flow of traffic is monitored. At the end of transmission destination node sends an acknowledgement via postlude message containing the no of data packets. Source node uses this information to check whether the data loss during transmission is within the tolerable range.

C. Mitigating routing misbehavior in self-organizing mobile ad hoc network using K-neighborhood local reputation system [8]

This paper presents a Novel reputation based mechanism to detect the misbehaving nodes (NRMDM). This system adopts the local reputation value of its K-hop neighborhood and the value is exchanged in K-hop neighborhood. This method helps to fully learn the experiences from its neighbor which helps to fully learn the experiences from its neighbor which helps to improve the ability to judge and improve itself. The node removal in MANET has continuity, so the node has to move their neighborhoods are. If the node record reputation of 1-neighborhood, when the node moves from the area, the reputation will be lost.

NRMDM consist four components as the Monitor, Reputation System, Path manager and the Witness module. Monitor module monitors the forwarding of the packets to the next node and caches the packet. The Reputation system calculates the rating of the node consists of reputation table and Reputation manager. The witness module observes unintentional dropping of packets and reports monitoring module.

D. Dynamic Trust Based Method to mitigate grey hole attack in mobile ad hoc networks [9]

The author proposed dynamic trust based method to mitigate gray hole attack. In this scheme each node calculates trust value and association status for all its neighboring nodes through monitoring its behavior in the network. To detect the malicious nodes, in this scheme each node maintains an association table. Association table is used to store the association status of any node with its neighbor table has two columns.

First the identifier or name of its entire neighboring node and relationship status with neighbor node. This table is referred every time when any node receives the packet status of the nodes can be according to their rating. If threshold value is than tanh value then node is assign a unknown node and labeled as malicious node.

E. A Novel approach for gray hole and black hole attacks in MANET [10].

In this paper an intermediate node detects the malicious node sending false routing information; routing packets are used not only to pass routing information. 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 route reply packets 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 node as malicious. Verifying nodes routing table; the node then tells other nodes not to consider the routing information received from the malicious node.

F. A Mechanism for gray hole attack detection in mobile ad hoc networks [11].

In this paper the algorithm eliminate the normal nodes with higher sequence the algorithm calculates the peak value and checks whether reply packet sequence number is less than or not. The parameter used to calculate the peak value, routing table sequence number, reply packet sequence number. In this structure in their local RAM which acts as a black list FALSE REPLY list of nodes. FALSE REPLY is the replies which are detected as a false from malicious node .depending on the number of FALSE REPLY from the node it decides to be black listed or not. Using this approach malicious node is added to black list and eliminates normal nodes to enter black list. Detection of malicious node is done during route discovery process. Whenever a malicious activity is detected by receiving node, it increases a false reply count for replying node in its local black list buffer (recv.node). Each node maintains its own black list buffer.

G. The impact of packet drop attack and solution on overall performance of AODV in MANET [12]

In this paper trusted list is used instead of black list. As the packet drop is minor attack as proved, to reduce re-analysis overhead analyzed node is added to trusted list. So it is skip that node's analysis in future. Trusted list is local to in local

RAM/buffer. Two counters are used one is count the total forwarded packets and second is count the total dropped packets of the replying nodes. Flag is set depending on condition for e.g. reliable flag is set to 1 and unreliable to 0. Reputation of route entry is the parameters used in algorithm to discard the packet from replying node.

H. Destination based group Gray hole attack detection in MANET through AODV [13]

In this paper when more than one malicious node are present in mobile ad hoc network than destination based algorithm is used. The algorithm contains three steps. In first step it stores the RREP packet on previous node. Second step checks 2 hop distance of a suspected node and third step contains the rejection of RREP packet. To identify the suspected node, the common neighbor of pervious node and suspected node checks the two hop distance node for reach ability to the destination. First it stores the RREP packet at previous node and attaches one hop distance of suspected node. When RREP message replies to previous node it should be also attach the one hop distance node of replying node otherwise previous node will reject the RREP message. If there is malicious node present in MANET then it send route reply (RREP) message to source by falsely replying that there is valid route.

I. Detecting black and gray hole attacks in MANET using an adaptive method [14].

This paper demonstrates an adaptive method to detect malicious node in MANET based on a cross layer design, in a network layer, a course-based method to overhear the next hop's action is proposed. This approach detects the node by modifying the detecting threshold according to the network's overload. In this scheme node does not observe every node in the neighbor, but only observes the next hop in current route path. Every node should maintain an FwdPacketBuffer, which is a packet digest buffer. When a packet is forwarded out, its digest is added into the FwdPacketBuffer and the detecting node overhears. Once the action that the next hop forwards the packet is overheard, the digest will be freed from the FwdPacketBuffer. In a fixed period of time, the detecting node should calculate the overhear rate of its next hop and compare it with a threshold. The overhear rate in the Nth period of time is defined as OR (N), the percentage of data packets which are actually received by the destination. This algorithm has some advantages like it does not send extra control packets secondly is routing packet overhead remains same.

J. Gray hole attack and prevention in MANET [15].

In this paper Intrusion detection system (IDS) is used to monitors the network or system activities for malicious activities or policy violation and produces reports to a

management station. Intrusion detection system aimed to securing the AODV protocol. In this system the extended protocol is proposed called is IDSAODV (Intrusion Detection System AODV).

CONCLUSION

Network security is the important and the biggest challenge for networks that are facing today. Gray hole attack is one kind of DOS attack which cause the damage and difficult to detect. More damage can be done when misbehavior nodes acts as normally in routing process and disrupt the network's operation. This paper provides the various detection scheme to detect the gray hole attack in MANET.

ACKNOWLEDGEMENT

I would like to express my deep sense of gratitude to my guide, Asst Prof.Vinit Kumar Gupta for his valuable guidance and useful suggestions. I would like to thank Asst Prof. Indr jeet Rajput also for his precious suggestion.

REFERENCES

[1] Ashok desai, " Review paper on detection and prevention techniques of gray hole attack in MANET ", in International journal of computer science and mobile computing, vol 2, issue 5, may 2013

[2] Rutvij H. Jhaveri, Sankita J. Patel, Devesh C. Jinwala, " Dos attacks in mobile ad-hoc network: A Survey ", second international conference on advanced computing and communication technology, 2012.

[3] G.s.Mamatha, Dr. S.C.Sharma, " Network layer attacks and defense mechanism in MANET- A Survey ", international journal of computer application volume 9, november 2010.

[4] Amit A. Bhusari, Pradeep M. jawandhiya, " Detection and Prevention techniques for gray hole attack in MANET ", international journal of computer applications X-PLORE 13.

[5] Amit N. thakare, Mrs. M.Y.Joshi, " Performance Analsis of AODV and DSR Routing Protocol in Mobile Ad Hoc Network ", IJCA special issue on " Mobile ad hoc networks", 2010.

[6] Gao Xiaoping, Chen Wei, " A Novel Gray Hole Attack Detection Scheme for Mobile Ad-Hoc Networks ", 2007 IFIP international conference on network and parallel computing- workshops.

[7] Sukla Banerjee, " Deteciton / Removal of cooperative Black and Gray hole attack in Mobile Ad-Hoc Networks ", proceedings of the world congress on engineering and computer science.

[8] S Neelavathy Pari, D. Shridharan ," Mitigating Routing Misbehavior in Self Organizing Mobile Ad hoc Network using K-neighborhood Local Reputation System" IEEE International Conference on recent trends in information technology.

[9] N.Bhalaji, A.shanmugan, " Dynamic Trust Based method to Mitigate Gray hole attack in Mobile Ad Hoc Networks", International Conference on Communication Technology and system design 2011.

[10] Rutvij j. Jhavri,Sankita J. Patel, Devesh C. Jinwala," A Novel Approach for Gray hole and Black hole Attacks in Mobile Ad Hoc Networks", second international conference on advanced computing and communication technology 2012.

[11] Ashok M. Kanthe , Ramjee Prasad, Dina Simunic," A Mechanism for Gray hole Attack Detection in Mobile Ad-Hoc Networks ", international journal of computer application(0975-8887) volume 53- no.16, september 2012.

[12] Ashok M. Kanthe , Ramjee Prasad, Dina Simunic,"The Impact of Packet Drop Attack and Solution on Overall Performance of AODV in Mobile Ad-Hoc Networks", international journal of recent technology and engineering (IJRTE) ISSN: 2249-8958, volume-2, issue-2, December 2012.

[13] Avenash Kumar, Meenu Chawla," Destination based group Gray hole ackttack detection in MANET through AODV", IJCSI international journal of computer science issue, vol-9 , issue 4, No 1, july 2012.

[14] Disha G. Kariya, Atul B. Kathole, Sapna R. Heda," Detecting Black and Gray hole Attacks in Mobile Ad Hoc Network Using an Adaptive Method ", international journal of emerging technology and advanced engineering, volume 2, issue 1, january 2012.

[15] Megha Arya, Yogendra Kumar Jain," Gray hole Attack and Prevention in Mobile Ad Hoc Network", international journal of computer applications(0975-8887) volume 27-No.10, August 2011.