International Journal of Electrical, Electronics and Computer Engineering **6**(1): 71-76(2017)

ISSN No. (Online): 2277-2626

A Review on Gray Hole Attack and its Prevention Mechanism

Ruchi Tiwari* and Jyoti Jain**

**M. Tech. Student, Electronic and Communication Department,*
Sagar Institute of Research and Technology Engineering R.G.P.V. Bhopal, (Madhya Pradesh), India
***Head of Department E &C Department,*
Sagar Institute of Research and Technology Engineering, Bhopal, (Madhya Pradesh), India

(Corresponding author: Ruchi Tiwari)
(Received 27 January, 2017 Accepted 05 March, 2017)
(Published by Research Trend, Website: www.researchtrend.net)

ABSTRACT: Wireless ad hoc network is extensively used for various applications such as military surveillance, scientific and industrial application due to its infrastructure less and dynamic behavior. In MANET each nodes act as a host or router, it means every node can send or receive the packets from the source to destination using routing protocols. This network may get compromise from severe type attack because of dynamic nature namely black hole, gray hole, wormhole, Sybil and byzantine attack etc. To prevent the network from these possible attacks various detection and prevention mechanism has been developed. In this paper, mainly focuses on the literature about the gray hole attack. This paper presents the merits and demerits of various gray hole attack detection techniques.

Keywords: Wireless Network, MANET, Gray hole attack, Infrastructure less

I. INTRODUCTION

Wireless ad hoc network is gaining popularity in various research areas such as military, scientific and industrial application due to its lack of centralization, dynamic topology and self-configurable behaviour. This is a kind of short durational network that does not have any managing authority which can produce a bunch of nodes that can communicate with one another with in a predetermined range of transmission. At this time the mobile nodes communicate directly with additional nodes without any router and hence the preferred functionalities are embedded to each node. Since the MANET comprises of mobile nodes with smaller number configurations of hardware and requirements compared to a router, hence protocols and routing used are of lightweight functionalities. Fig.1. shows that nodes in MANETs can move independently and their path changes from node to node. In MANET each node is able to send and receive the routing request, so it can act as host or router.[1] But due to dynamic topology, lack of central monitoring (infrastructure less) and need for cooperation makes MANETs more vulnerable [2]. These vast features become serious problems regarding the security point. Particularly, if the existence of malicious nodes may disturb the routing process that cause gray hole attack to defect in the network. With the increase in the use of MANETs, security becomes a key obligation to provide communication among the mobile nodes [4].

The routing protocol in MANET is categorized in two types: Proactive and Reactive. This effort deals with enhancing MANET security using intrusion detection system for the AODV reactive protocol. The nodes that work towards degrading the ordinary network performance are called as malevolent or attacker nodes. The sort of traffic generated by such node is malicious and influences the lifetime of network and other performance factor. Also the intruder's nodes intend towards the modification of authentic packet information and counterfeit them for diverting the network traffic through these malicious nodes which later on dropped or delayed. For the period of the last few years, many approaches had been suggested along with several intrusion detection systems. Though there are a few problems which stay unaddressed and are not resolved as required. In the presence of these nodes or in delays of such detection the network performance gets down continuously. Gray hole attack is one of the attack in network layer which comes under security attacks. A disparity of black hole attack is the gray hole attack, in which the nodes will drop the packets selectively. In this paper, we presents the literature study about the gray hole attack detection and prevention.

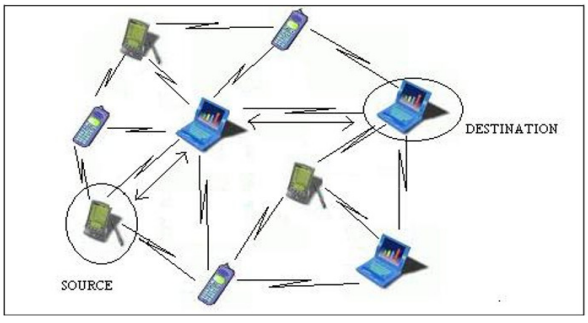

Fig. 1. Mobile ad hoc network.

A. Security Goals

In MANET, all networking functions such as routing and packet forwarding, are performed by nodes themselves in a self-organizing manner. For these causes, securing a mobile ad -hoc network is exceptionally challenging. The goals to evaluate if mobile ad-hoc network is secure or not are as follows:[4]

-Availability: Availability means the assets are available to authorized parties at apposite times.

This applies both to data and to services. It makes sure the survivability of network service despite denial of service attack.

-Confidentiality: Confidentiality makes certain that computer related assets are accessed simply by authorized parties. Fortification of information which is exchanging through a MANET. It should be protected against whichever disclosure attack like eavesdropping- unauthorized reading of message.

-Integrity: Integrity means that devices can be modified only by authorized parties or simply in certified way. Integrity guarantees that a message being transferred is never corrupted.

-Authentication: Authentication is effectively guarantee that participants in communication are legitimated and not impersonators. The recourses of network should be accessed by the authenticated nodes.

-Authorization: This property assigns unusual access rights to diverse types of users. For instance a network management can be performed by network administrator merely.

-Resilience to attacks: It is required to prolong the network functionalities when a fraction of nodes is compromised or destroyed.

-Freshness: It makes sure that malevolent node does not resend formerly captured packets.

The organization of rest section of research paper is done in this manner: In section 2 gives brief description about different types of attack which influence the performance of the wireless network. Section 3 presents the gray hole attack in wireless ad hoc network. In section 4 discusses the literature study about the former work done by the various authors or researcher to combat/ thwart the gray hole attack. In last section concluded about the overall paper with future work.

II. SECCURITY ATTACKS

Mobile Ad hoc networks are vulnerable to various attacks not simply from outside but also from inside the network itself. Ad hoc network are mostly subjected to two diverse levels of attacks [5]. The first level of attack occurs on the basic mechanisms of the ad hoc network such as routing. While the second level of attacks tries to harm the security mechanisms employed in the network. The attacks in MANETs are divided into two major types like Internal and External attacks.

A. Internal Attacks

Internal attacks are directly leads to the attacks on nodes presents in network and links interface between them. This variety of attacks may broadcast erroneous type of routing information to other nodes. Internal attacks are sometimes more complicated to hold as compare to external attacks, since internal attack occurs due more trusted nodes. The false routing information spawned by compromised nodes or malevolent nodes are indicated to identify. This can be due to the compromised nodes are able to spawn the legitimate signature using their private keys.

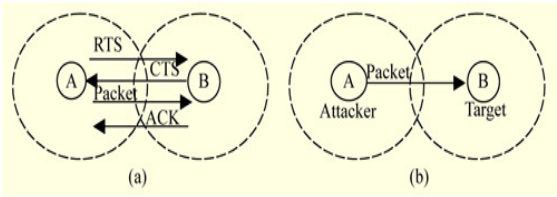

Fig. 2. Internal Attack.

B. External Attacks

External attacks are carried out by nodes that do not belong to the network. It causes congestion sends false routing information or causes unavailability of services. These types of attacks try to cause congestion in the network, denial of services (DoS), and advertising counterfeit routing information etc. External attacks thwart the network from ordinary communication and producing additional overhead to the network. External attacks can classify into two categories like active and passive attacks.

Passive Attack. This attack won't interrupt the normal operation of MANET, while data have been exchanged from the network [6]. The solely nature of passive attack is to identify the data exchanged in the network [8]. The attacker snoop the data exchanged in the network without altering it. Here the requirements of confidentially gets violated. One of the resolutions to the difficulty is to exploit powerful encryption mechanism to encrypt the data being transmitted, thereby making it impossible for the attacker to get useful information from the data overhead [7]. There are two different kinds of attacks in the Passive attacks they are Eaves Dropping and Traffic analysis Monitoring. These are the two attacks which take placer currently in the passive attack. Other than when we employ a powerful encryption method we can diminish the problem. Generally in the passive attack the task of the network is to monitor and analyze which type of communication is going on [9]. Here the Traffic analysis adversaries monitor packet transmission to infer important information such as a Source, destination and Source- destination pair [11]. Eavesdropping is another kind of attack that usually happens in the mobile adhoc networks.

It aims to obtain some confidential information that should be kept clandestine during the Communication. The information may comprise the location, public key or even passwords of the nodes [10]. As such data is extremely much useful and central to the security state of the nodes; they should be set a side from the unauthorized nodes.

Active attacks. An Active attack always tries to modify the normal operation of MANET, which means the inter rule have been made in the network, for instance doing data interruption, modification, exposure and fabrication. Active attacks can be internal or external. The information which is routing through the nodes in MANET is altered by an attacker node. The attacker node also streams some counterfeit information in the network. Attacker node also do the task of route request though it is not authenticated node so the other node discarding its request because of these route requests the bandwidth is consumed and network is jammed [12]. Some of the security threats in the networks are Interruption, Interception and Adaptation. Some of the significant active attacks are follows, they are Grayhole attack, Black hole attack, Worm Hole attack, Information disclosure and Routing attacks. These attacks can be happened at any point of time in the network. So it is very much necessity to avoid such attacks in the network. Since it is very hard to find and detect these kinds of attacks, we need to rectify the problem by some of the powerful encryption techniques.

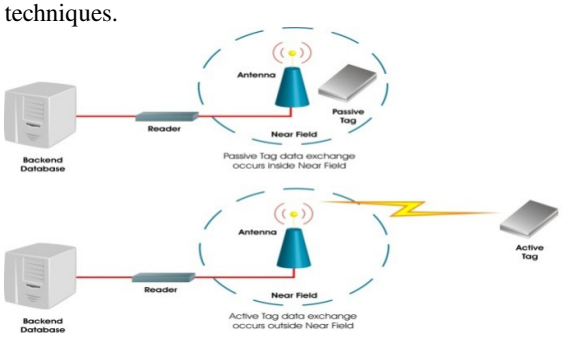

Fig. 3. Active and Passive Attack in MANET.

III. GRAY HOLE IN MANET

Gray hole is one of the attacks found in ad hoc network which act as a slow poison in the network side it means we cannot suppose how much data can be lost. In gray hole Attack [13] a malicious node trashes to precede certain packets and simply drops them. The attacker selectively drops the packets beginning from a lone IP address or a range of IP addresses and forwards the remaining packets. Gray hole nodes in MANETs are very effective. All node preserve a routing table that holds the next hop node information for a route a packet to destination node ,when a source node want to route a packet to the destination node, it uses a meticulous route if such a route is available in its routing table. If not, nodes initiate a route discovery process by broadcasting Route Request (RREQ) message to its neighboring nodes. By getting the RREQ message, the intermediary nodes bring up-to-date their routing tables in a reverse route to source node. A Route Reply (RREP) message is sent backward direction of the source node after the RREQ query reaches either the objective node itself or any other intermediary node that has a recent route to destination. Now we define the gray hole attack[14] on MANET'S. The gray hole attack has two significant phases.

In primary phases, a malevolent node exploits the AODV protocol to proclaim itself as having a valid route to destination node, with the intension of interjecting or humiliating packets, even though route is counterfeit.

In second phases, the malicious nodes drop the intermittent packets with a certain prospect. The process of finding gray hole is very challenging task. In certain new grayhole attacks the attacker node acts maliciously for the duration until the packets are dropped and then switch to their ordinary nodes behavior. By these activities it's very challenging for the network to distinguish such kind of attack. In some cases grayhole attack is also called as node misbehaving attack. The discrepancy of black hole attacks is the grayhole attack, in which the affected nodes either drop packets selectively. Both categories of grayhole attacks look for to unsettle the network without being detected by the security measures in place [15].

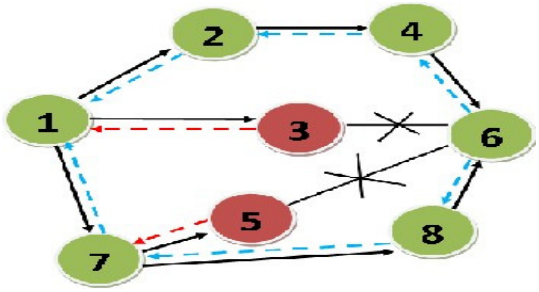

Fig. 4. Gray Hole Attack in MANET.

A. Solutions of Grayhole Attack

The Use of Modified Extended Data Routing. Information Table The discovery and exclusion of assistance black hole attack and grayhole attack by fixing the MEDR(Modified Extended Data Routing) in any given node is part of(the contents of) the table not only to discover a malevolent node but not a modify in the history of his preceding destructive behavior gray help hole has been used as a method protocols Ad Hoc (case) have selected for algorithm design and

development program and meet the requirements of AODV protocol [22].

Tree Merkel. Using Merkel tree [23] to detect gray hole attacks will be discussed. Merkle tree is a binary tree, each leaf of a credit number and license number of intermediate nodes of credit, to create a new combination number. This method can also cooperate with each other as well as black holes attacks to the [22].

Use of Guess the Sequence Number. In this way, each network node is required due to the nature of network traffic, the maximum number of sequences may presume, and when receiving a call packet routing, the highest sequence number with the sequence number response packet compare; If number the sequence number of response was more, node sending it malevolent in its working principles, techniques based on guessing the sequence number. If the received packet sequence number is exceeded, the value of the packages marked as malevolent node and sends it to the subsequent node; to other nodes in the directory as a malevolent and node sending the call as a malicious node title mark. Methods that are based on the sequence number guessing attacks by a malicious node are complicit and in attacks collaborationist nodes, cannot detect all the malicious node and only manufacturer of the node package will be identified. It also has an elevated processing overhead for the whole network, because since each node in the network must persistently determine the maximum sequence number and the sequence number of the received packet compare [24].

IV. RELATED WORK

This section of the paper, presents the literature about the earlier work in the detection and prevention of the gray hole attack which are describing below

Authors/Researchers	Descriptions	Tools	Parameters	Publishing Year
Kumar & Dushan [2]	Proposed solution considered this deployment approach for detection and built a solution to using IDS-agent approach to detect highest sequence number node. When it detects the suspicious node, it adds it into blacklist of source node to avoid further transmission	NS-2	PDR, E2E, Throughput	2016
Rana & Mittal [15]	Watchdog mechanism proposed in is a monitoring method used for wireless sensor networks, and is the basis of many misbehavior detection algorithms and trust or reputation systems.	NS-2	remaining energy, Average end to end delay, Distinct event delivery ratio, and number of collisions	2016
Dumne and Manjaramkar [1]	Proposed a method to resolve this problem by using malicious node detection schema based upon DSR mechanism -cooperative bait detection scheme (CBDS) which uses hybrid defense architectures. CBDS technique helps to find out malicious node by using a reverse tracing technique	NS-2.35	Throughput, PDR	2016
Chundong She[17]	Suggested a path-based scheme to overhear the next hop's action. In this method, a node does not observe every neighboring node, but only observes the next hop in recent route path. each node should keep a packet digest buffer say FwdPktBuffer. Whenever a packet is forwarded to, its digest is added into the FwdPktBuffer and the detecting node overhears. Once it is overheard that the next hop forwards the packet, the digest will be released from the FwdPktBuffer. The detecting node should calculate the overhear rate of its next hop in a fixed period of time, and compare it with a threshold. Author define overhear rate as (total overheard packet no/total forward packet no).	NS-2	Detection Rate and False Positive Rate	2010
Khattak et al. [17]	Use the second optimal route for data packets transmission and hash function for black and gray holes attacks avoidance and data integrity	NS-2	Delay ,Throughput	2013
Dharman and Venkatachalam [18]	Proposed a gray hole attack Detection technique the using second shortest route to destination and message digest based technique	NS-2	Packet Loss, PDR,E2E, Routing Load	2016
Khattak and Nizamuddin [19]	Presented a hybrid approach for preventing black/gray hole attacks by selecting second shortest route for secure route selection and hash function and timestamp base solution for consisting data transmission.	NS-2	Delay, Throughput	2013
Soliyal and Bhadauria [20]	Analysed nature of packet dropping and bandwidth attack based on AODV routing protocol on MANET, and proposed node bypassing technique to detect gray hole attacks	NS-2	Throughput, PDR,	2016

V. PROPOSEDMETHDOLOGY

Proposed method is based on calculation of Packet Drop Ratio (PDR) of network to detect gray hole node. For this calculate the value of PDR and detect the suspicious activity in network nodes after every 10 second interval to detect gray hole behavior.

Step1-Calculate Packet Drop Ratio (PDR) of network.

Step 2- Check performance of network continuously Find the PDR decreasing or not.

Step 3- If PDR decreased it means any suspicious node is present in the network .

Then call Blacklisted function to remove the suspicious path.

Blacklisted that suspicious path.

step 4- Route discovery phase -

Find a new fresh route to send the data packets from source to destination.

Step 5- Check radio range of nodes in the network.

If radio range>550 m^2

then we will not communicate with such type of nodes.

And nodes are unreachable out of this range.

Else radio range <550m^2

Communication is possible .

Step 6- Check avg time

Δ = (received time-sent time) $\times 100$

If Δ is decreased.

Then will check again such type of malicious node activity.

Process repeated continuously in each 10 second.

Blacklisted the route.

Call route discovery**.**

VI. CONCLUSION

Wireless ad hoc network is dynamic and infrastructure less network and because of this various kinds of security threats compromises from the nodes and these misbehaving nodes cause severe damage over the network such as packet drop and bandwidth. Gray hole is one of the security threats compromises from the nodes and these misbehaving nodes cause severe damage over the network such as packet drop and bandwidth. Gray hole is one of the security threats of network layer which perform selective pack dropping. To combat this attack various techniques has been proposed and developed. In this paper, we presents the literature work for the mitigation of gray hole attack by various researcher. After reviewing these method analyzes that some approaches are efficient in improving the performance in case of PDR and throughput and some consumes less bandwidth but they decreases the throughput. So in future work, design a hybrid approach which will improve the performance with respect to bandwidth, throughput, PDR and delay also.

REFERENCES

[1]. Pradeep R. Dumne, Arati Manjaramkar "Cooperative Bait Detection Scheme to prevent proceeding of IEEE.

[2]. Sudheer Kumar, Nitika Vats Doohan "A Modified Approach for Recognition and Eradication of Extenuation of Gray-Hole Attack in MANET using AODV Routing Protocol", Symposium on Colossal Data Analysis and Networking (CDAN), 2016 in proceeding of IEEE.

[3]. S. Corson and J. Macker, RFC 2501, "Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations," Jan. 1999.

[4]. C. Suhashini, S. Sivakumar "A Secure Approach with Physical Layer Encryption in MANET", *International Journal of Innovative Research in Science, Engineering and Technology*, ISSN ONLINE(2319-8753)PRINT(2347-6710).

[5]. R. Divya Paramesvaran, Dr. D. Maheswari "Study of Various Security Attacks in Network Layer and the Mitigation Techniques for MANET", *International Journal of Advanced Research in Computer and Communication Engineering* Vol. **5**, Issue 2, February 2016. ISSN (Online) 2278-1021.

[6]. A. Saini, R. Sharma, "A Study of various Security Attacks & their countermeasures in MANET" IJARCSSE, vol.**1**, Issue.1, Dec 2011.

[7]. Dhamande C.S and Deshmukh H.R "A Competent to diminish the brunt of gay hole attack in MANET" Vol.**2**, Issue 2 Mar 2012.

[8]. Stephen Carter and Alec Yasinac "Secure Position Adhoc Routing"

[9]. M. Wazid, Rajesh Kumar Singh, R.H.Goudar, "A Survey of Attacks Happened at Different Layers of Mobile Ad- Hoc Network & Some available Detection Techniques" IJCA , Vol. **3**, No,2 Feb 2011.

[10]. Z. Zhao, Hongxin Hu, Gail-JoonAhn and Ruoyu Wu "Risk Aware mitigation for MANET Routing attacks" *IEEE Transactions on Dependable and Secure Computing* Vol. **9**, No.2 Mar/Apr 2010.

[11]. Pradip M. Jawandhiya, Mangeshm. Ghonge, DR. M.S Ali and Prof. J.S Deshpande " A Survey of Mobile adhoc network attacks" Vol.**2**, No.9, Sep 2010.

[12]. V. Solomon Abel, "Survey of Attacks on Mobile Ad-Hoc Network" *IJCSE*, Vol. **3**, No.2, Feb 2011.

[13]. Vishnu K, and Amos J. Paul, "Detection & Removal of cooperative Black/Gray hole attack in Mobile ADHOC Networks." *International Journal of Computer Applications 2010*, Volume **1**, No.22, pp.38-42. Sukla and Banerjee "Detection/Removal of Cooperative Black and Gray Hole Attack in Mobile Ad-Hoc Networks" *Proceedings of the World Congress on Engineering and Computer Science 2008 WCECS 2008*, October 22 - 24, 2008, San Francisco, USA.

[14]. Oscar F. Gonzalez, God win Ansa, Michael Howarth and George Pavlou. "Detection and Accusation of Packet Forwarding Misbehaviour in Mobile Ad-Hoc networks", *Journal of Internet Engineering*, **2**: 1, 2008.

[15]. Ankita Rana, Er. Ankita Mittal "A Mechanism For Detection and Prevention of Multiple Gray Hole Attack In Wireless Sensor Networks", IJARIIE Vol-2 Issue-1 2016, ISSN (O)-2395-4396.

[16]. Jiwen CAI, Jialin CHEN, Zhiyang WANG, Ning LIU, "An Adaptive Approach to Detecti Black and Gray Hole Attacks in Ad Hoc Network", IEEE International Conference on Advanced Networking and Applications, 2010.

[17]. Chundong She, Ping Yi, Junfeng Wang, Hongshen Yang "Intrusion Detection for Black Hole and Gray Hole in MANETs"*KSII Transactions on Internet and Information Systems*, Vol. 7, no. 7, jul. 2013.

[18]. V. Dharman, G. Venkatachalam "Detection of Gray Hole Attack in AODV for MANETs by using Secure Message Digest", *South Asian Journal of Engineering and Technology,* Vol.**2**, No.17 (2016) 321–329, ISSN No: 2454-9614.

[19]. Hizbullah Khattak, Nizamuddin "A Hybrid Approach for Preventing Black and Gray Hole Attacks in MANET", In proceeding of IEEE-2013.

[20]. Neema Soliyal, H. S. Bhadauria "Preventing Packet Dropping Attack on AODV Based Routing in Mobile Ad-Hoc MANET", Intl. Conference on Advances in Computing, Communications and Informatics (ICACCI), Sept. 21-24, 2016, Jaipur, India.

[21]. Hiremani. Vani A, Jadhao. Manisha Madhukar, "Eliminating Co-operative Black hole and Gray hole Attacks Using Modified EDRI Table in MANET", IEEE, 2013.

[22]. Merkle, R. C. (1988). "A Digital Signature Based on a Conventional Encryption Function"."Advances in Cryptology CRYPTO '87". Lecture Notes in Computer Science 293. p. 369. doi: 10.1007/3-540-48184-2_32. ISBN 978-3-540-18796-7,1988.

[23]. Doori. Ali, Mohammad Karimizadeh Takabi. Tahereh, "Black hole attack analysis and network discovery in MANET ", Regional Conference on Electrical and Computer Engineering methods of calculation software, Islamic Azad University Safashahr, February 2014.(in persian).