American Journal of Software Engineering and Applications
2016; 5(3-1): 15-19
http://www.sciencepublishinggroup.com/j/ajsea
doi: 10.11648/j.ajsea.s.2016050301.14
ISSN: 2327-2473 (Print); ISSN: 2327-249X (Online)

Methods for Detection and Removal of Grayhole Attack in Mobile Adhoc Network (MANET)

Mahdi Zolfaghari[1, *], Mohammad Sadeghzadeh[2], Reza Frouzande[1], Ahmad Emami[1]

[1]Department Computer, Science and Research Branch, Islamic Azad University, Tehran, Iran

[2]Department of Computer, Mashhad Branch, Islamic Azad University, Mashhad, Iran

Email address:

Mahdi.zolfaghari.ir@gmail.com (M. Zolfaghari), sadeghzadeh.edu@gmail.com (M. Sadeghzadeh), r.frouzande@gmail.com (R. Frouzande), ahmademami67@gmail.com (A. Emami)

[*]Corresponding author

To cite this article:

Mahdi Zolfaghari, Mohammad Sadeghzadeh, Reza Frouzande, Ahmad Emami. Methods for Detection and Removal of Grayhole Attack in Mobile Adhoc Network (MANET). *American Journal of Software Engineering and Applications.* Special Issue: Advances in Computer Science and Information Technology in Developing Countries. Vol. 5, No. 3-1, 2016, pp. 15-19. doi: 10.11648/j.ajsea.s.2016050301.14

Received: March 6, 2016; **Accepted**: March 7, 2016; **Published**: June 24, 2016

Abstract: Mobile Adhoc Networks, because collections of moving node and wireless is formed and also due to the dynamic changes in the communication topology, which is quite vulnerable target a wide range of attacks were shown; one of the attacks, Gray hole attack that is easy on reactive routing protocols such as Dynamic Source Routing protocol runs out. Gray hole attack, not the malware behavioral honest during the process of discovery route, but later, the malicious node is leveling; and can route discovery process to transmit information on the network, stirred and network performance to reduce the loss of data. Therefore using this method of detection and removal of malicious attacks, is useful to increase network efficiency and ensure correct data in ad hoc networks is transmitting. In this paper we introduce the attack and investigate the last gray hole existing methods for detecting and removing it is addressed. The paper is concluded with discussion on the results.

Keywords: Mobile Adhoc Network (MANET), Gray Hole Attack, Dynamic Source Routing (DSR), Black Hole Attack

1. Introduction

Ad hoc network that dynamically moving a decentralized network, without infrastructure and temporary free and mobile nodes are intermediate nodes; in the network operating as a router worked and done and messages sent from one node to another [1].

Gray hole attack [2], which is also called selective Black hole attack [3]; Is a certain type of Black hole attack in which a malicious node is not the first malware, malicious node later [4]. The attack malicious nodes to properly participate in the discovery process, but when between them, a route chosen to send to exist; they are selectively removed and the packet will Board [5].

Dynamic source routing protocol [6], on demand, which act performs routing of origin, the sender of the path that must be taken step by step to the destination, is aware. If there are multiple paths from source to destination, these routes are stored in the cache. Field path from source to destination in the packet header is maintained [7].

Black hole Attacks [8], which is one block attacks known to be the malicious node, network traffic directed to your hand after receiving data packets, all packets destroys [9].

Black hole attack, a malicious node can request a new route every packet by mistake or shortest route to the destination, and then they will attract to their side without sending it to pepel, while in gray holes attack, malicious nodes to properly participate in the discovery process; but once a route to reach the destination is selected, they are selectively removed packet. In this reason only a part of packets removed. Detect Gray hole attack is much more difficult to attack the black hole [5].

So thorough familiarity with new and useful methods of detection Gray hole attack, and finally remove the gray hole attack can cause destruction ad hoc networks is animated by the challenge security, and the result increases and improve network performance as well as increases productivity and prevents data loss.

2. Related Work

In this section we investigate previous work on Mobile Adhoc Networking of the Gray hole attack animation in the Mobile Adhoc Networks.

2.1. Mobile Adhoc Networks and its applications

Mobile Adhoc Networks, a network without infrastructure and ability to configure the mobile devices that are connected through wireless links have been formed. Each device in a MANET is free to move independently in any direction and thus links it to other devices, which constantly changes. Mobile devices including routers and hosts, make up an arbitrary graph. MANET networks may operate independently or be connected to another network such as the Internet [10]. The applications of Mobile Adhoc Networks include:

- General applications
  The relationship between public vehicles and taxis
- Military applications
  Fields of war, the army and the war fleet communications
- Personal applications
  Connect laptop computers with each other
- Emergency applications
  Flood and earthquake rescue operations etc [1, 3, 5].

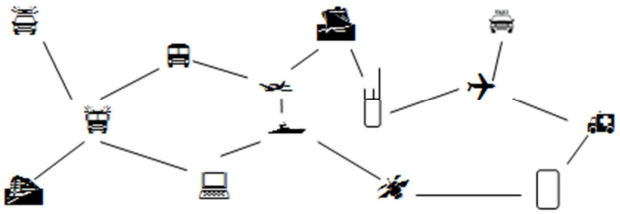

Figure 1. *The application and architecture Mobile Adhoc Network.*

2.2. Gray Hole Attack

Gray hole attacks knots can cause in three directions:

1) Malicious node while the rest of the package returns the specified packets from node to bring down and destroy.

2) A node can be identified in time, destructive behavior, and optional packages fall and destroy.

3) Both attacks (black hole and gray hole) merge with each other, for example, a malicious node may fall in a given period of time specified node and destroy. Then the node is in a normal state. Because of these features, it is very difficult to detect Grey holes attacks. Grey holes and black holes attacks can be easily both on-demand distance vector routing protocols such as routing response on the application and run dynamic source routing [5].

A node will not be able to see all the nodes in his neighborhood, but only will be able to watch the next jump in the current direction. S is the source node and the destination node D, and node A is a black hole. Node S is sending data packets to node D through the D, B, A, S is. In this design, only node A to node S will be able to see the next jump and will be able to take care of Units 1 and 2, [11].

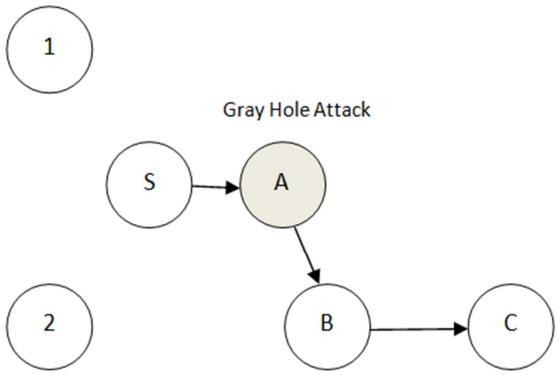

Figure 2. *Gray Hole Attack [11].*

3. Methods of Detection and Removal of Gray Hole Attack

This article reviews the newest methods of attack detection and removal of gray hole attack

3.1. The 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 guess, and when receiving a call packet routing, the maximum sequence number with the sequence number response packet compare; If number the sequence number of response was more, node sending it malicious. in its working principles, methods based on guessing the sequence number.

If the received packet sequence number is exceeded, the value of the packages marked as malicious node and sends it to the next node; To other nodes in the directory as a malicious 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, can not detect all the malicious node and only manufacturer of the node package will be identified. It also has a high processing overhead for the entire network, because since each node in the network must constantly calculate the maximum sequence number and the sequence number of the received packet compare [9].

3.2. The Use of Modified Dynamic Source Routing Protocol

In this way, when the source node has data packets to send to the destination, the data that is to be transmitted into different Division of blocks and sends at a time of the blocks of data to the destination; It also the number of data packets that it sends to destinations in a block before the actual transmission of data used a different route (The second shortest path to reach the destination).

It starts process of discovering the gray hole attacks. First sends a Query Request (QREQ) packet to node in the source route (Forwarding path to data) at between 2-hop form it distance. QREQ to find the number of data packets sent to the same node to the node can be used to jump to the next; node-1 package an answer, initially to the node (QREP) sends to the

destination D. QREP includes a number of data packets sent from the node contains a jump to the next adjacent route origin. The destination node using QREP receives that confirmation of whether the previous jump, her neighbor (for example an node) all packages node of your data that is received from the previous (an node-1) to correctly post; if true is not the destination node will send both an and an-1 node-to-node sends the suspect list. If you are sending the correct means that these two nodes are in the correct functioning of the data submitted. Therefore, the destination node is again a new QREQ node sends an-3 at a distance of 2 jump from an node-1 offset path. The destination node using QREP receives that confirmation of whether two nodes and an-3-2, all of which have received data packets correctly. This process will continue until QREQ to reach major who has a previous path nodes to a distance of 2 jump in the path may not be offset. (Figure 3-a) GN QREQ package to the destination node (the node the gray cavity) that sends at a distance of 2-hop of the destination node. Malicious node information in the form of GN being properly on how to send the packet to the next node doesn't send (Figure 3-a).

In (Figure 3-b) node 1 and 6 respectively the source and destination are the same. If for example the source node will send 100 packet, and the destination node only 60 packages of it receives, the destination node 4 node a sends to QREQ. QREP package that contains the node 4 number of packets (in this example 60 packets) to the next node (node 5) resend. 5 node Pack QREP destination node received and 6 forwards. 6 node confirms that the number of packets received from 5 knots with the number mentioned on the Pack of matches but QREP realizes that node a 4 Pack only 60 out of 100 packets sent by the source node forwards again so 4 nodes to list nodes suspect pass; then a packet to node 2 QREQ at a distance of 2-hop (2 jump) of 4 nodes located Added. Node 2 is a number containing QREP packets (Pack of 100) that the next node to the node instance sends the GN sent. QREP GN node has received the package and sends them to the destination again. Malicious node could not modify QREP GN closed because messages with identity verification code (MAC), which is connected with the private number of nodes (node 2) and random number to reduce the risk of attack has been prepared. At the same time get the destination node, view by QREP that the number of outgoing packets from node to node 2 GN 100., while node 4 send real depending 60. so it is likely that both GN and knot 2 remove packages and information sent by the node 2 is also false. Hence, the destination node of the node 2 and node list mentioned in the suspicious GN are [5].

Now the destination node, intimate the suspected the nodes in the source route to private node IDS as MNREQ package (ask the suspect node) is introduced. Package IDS to all nodes again MNREQ. only by a node IDS MNREQ package to an adjacent node IDS added. after a period (interval to get IDS by all nodes MNREQ, node IDS that are in the vicinity of the source node, the source node ALARM package to send to it the presence of attackers are on track to post data, and aware of them wants the block Send your information to the next;

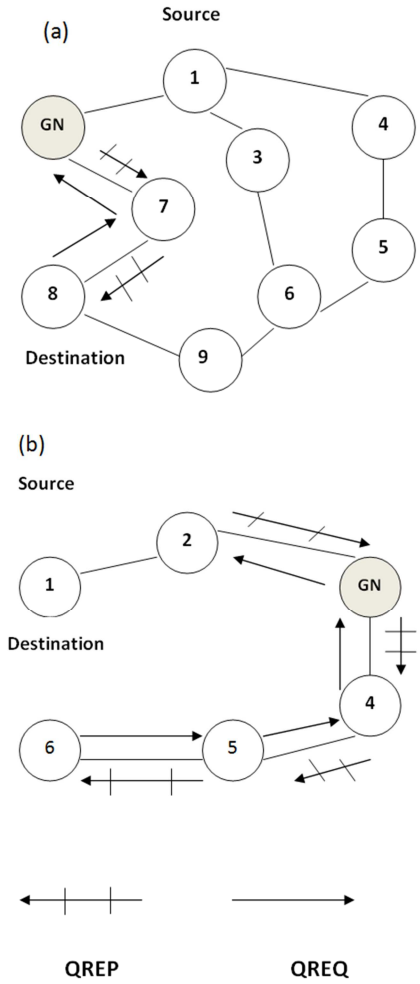

Figure 3. *QREQ and QREP Transmission between nodes in source route at 2-hop distance. [5].*

When the source node sends the next information block, node IDS that were suspicious in the vicinity of the node to become destructive mode and ears that are packets sent or deleted by a suspicious node can accept. If any of the nodes of the suspect were found deliberately remove the packets, rather than in the list of nodes that are suspected; then the node IDS shown, a blocking message to all nodes of the near post. Each node IDS after receiving the message blocker it moves to your neighbors and thus suspicious node will be removed. Message blocker only by the node IDS in the network. Each node, upon receiving a blocking message from the malicious node data-aware, and then delete the message without the forward, Once you locate the suspect node and removed all of the nodes of any routing information consists of the nodes of the carriers have come and there is no malicious node could not be replaced include the RREP [5].

3.3. The use of Prime Product Number

Prime Product Number (PPN) proposal to reduce the adverse effects of malicious nodes. The basic idea is that PPN plan, each node in the network can be a specific number of nodes act as its identity and this identity is not possible to change methods of PPN as a supplement

protocol AODV (Ad hoc On Demand Distance Vector) routing Case (Adhoc) PPN-based programs can be effective AODV and malicious node attacks formed between the source and destination stop along the way. PPN program of distance-vector routing required on the demand for road use during the process.

PPN in each node, the cluster has the task of maintaining a neighboring table to hold information about all the nodes in the discovery phase of PPN program used an intermediate node will attempt to create a pathway along A node that does not use the information he is wrong and PPN fully do so, gradually malicious node in the network nodes will avoid destroying other [4].

3.4. The Use of Modified Extended Data Routing Information Table

The discovery and removal of cooperation projects blackhole 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 malicious node but not a change in the history of his previous 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 [3].

3.5. The Use of Intrusion Detection Systems

All intrusion detection systems by implementing a mechanism called ABM (anti-Blackhole mechanism) is mainly used for the estimation of the value of the SAR () being a node based on an unnatural amount of the difference between RREQs and RREPs of the sent node.

When the amount of SAR more than a predefined threshold is a block of a message by IDS, to inform all the nodes in the network are broadcast will be sent together to isolate malicious node. Block message, containing the node IDS issued and identify the black holes and time identifying it. As soon as they get the message blocks issued by IDS, typical of malicious nodes in places black list put their [12].

3.6. The use of Watchdog Technique

Watchdog Technique [13] or timer watch, packet-based method to detect malicious node misbehavior, move forward or lost depending on the period of time that is specified, is; Be the timer to count a time for transmitting packets from the source node to the destination node [3].

Watchdog Technique is one of the basic methods that presumably many intrusion detection method that has been created there.

Malicious node on the next jump, by eavesdropping (covert listening) through sentinel detection methods are diagnosed. The routing path that we wanted to help in some way that it is possible to identify the malicious nodes also be included.

The dynamic source routing protocol routing data at the source node is defined. This information is transmitted in the form of a message to the intermediate nodes until it reaches the desired destination. Therefore, each intermediate node in the node where the next jump there must recognize. Moreover, due to the specific characteristics of wireless networks may be used to hear the message the next jump.

For example, if node A is near node B, then node A can hear node B communications.

Assume that node S (source) wishes to send a packet to node D (destination). A route through A, B and C of Node source S to the destination node D there. Imagine now that node A before the data packet at the source node S to the destination node D had received. And to ensure that data packets to Node C Node B is moving forward. If the node B (with dotted lines) data packet eavesdropping and surveillance information, and sends the same to what is in its buffer.

Node B indicates that the data packet to the node C (the solid line) is moving forward. The data package has been removed from the source node buffer. On the other hand closed in a time source node with packet buffer is not comparable approach to identify sentinel node B, adds the error counter. If the number of the counter is more than the threshold node A, node A concludes that node B, node to node, the source S malicious reports [14].

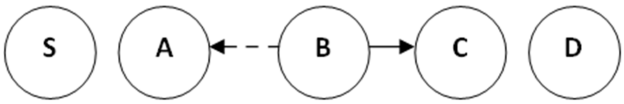

Figure 4. *Watchdog Technique [14].*

3.7. The use of tree Merkel

Using Merkel tree [15] 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 [3].

Table 1. *Check the number of methods to detect and remove Gray Hole Attack.*

Detection and removal of Gray Hole Attack	Advantages and Disadvantages
guess the sequence number	high overhead [9]
modified Dynamic Source Routing protocol	high overhead [5]
Prime Product Number	avoid malicious nodes in the network of non- malicious[4]
Modified Extended Data Routing Information Table	Constantly modified extended on the routing information[3]
Intrusion Detection Systems	energy consumption high, Resend data packets, difficult application and challenging[12]
Watchdog Technique	Decrease overhead[14]
tree Merkel	Constantly intermediate node to leaf node[3]

4. Discussion and Conclusion

Mobile Adhoc Networks is progressing rapidly in case because with increasing motion devices, portable and inexpensive that performance and have more power and slightly rising are a must in terms of the quality of the time are the most important consideration; Therefore an important challenge for Mobile Adhoc Network security item and is one of the network's security vulnerabilities, Gray Hole Attack which causes the destruction of the networks and reduce efficiency and loss of information and data, increased energy consumption; Therefore necessary familiarity with methods to detect and remove the Gray Hole Attack and finally remove this security challenge is an important issue which is very important; Hence it is necessary to express that this method of detect and remove for the other attacks and can be security challenges not only for the Mobile Adhoc Networks but also to other subsets of Adhoc Networks networks but also to other subsets like to use.

References

[1] Khattak. Hizbullah, Nizamuddin, "A Hybrid Approach for Preventing Black and Gray Hole Attacks in MANET," 978-1-4799-0615-4/13/$31.00, IEEE, 2013

[2] 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. 38-42.2010

[3] Hiremani. Vani A, Jadhao. Manisha Madhukar,"Eliminating Co-operative Blackhole and Grayhole Attacks Using Modified EDRI Table in MANET", IEEE, 2013

[4] Gambhir. Sapna, Sharma. Saurabh, "PPN: Prime Product Number based Malicious Node Detection Scheme for MANETs", IEEE, 2012

[5] Mohanapriya. M, Krishnamurthi. Ilango, "Modified DSR Protocol for detection and removal of selective black hole attack in MANET", ComputElectrEng(2013), http://dx.doi.org/10.1016/j.compeleceng.2013.06.001, Elsevier, 2013

[6] D. B. Johnson and D. A. Maltz. "Dynamic Source Routing in Ad Hoc Wireless Networks," Mobile Computing, edited by Tomasz Imielinski and Hank Korth, Kluwer Academic Publishers, chapter 5, pp. 153–181, 1996

[7] Mazidi. Arash, Rajabzade. Mostafa, "Analysis, assessment and implementation of routing algorithms in ad hoc networks", the Eighth Symposium on Advances in science and technology, computer engineering and sustainable development with a focus on computer networks, modeling and security systems, higher education institution grave, Mashhad, December 2013. (in persian)

[8] M. Al-Shurman, S.-M. Yoo, and S. Park, "Black hole attack in mobile adhoc networks," in Proceedings of the 42nd annual South east regional conference. New York, NY, USA: ACM Press, pp. 96-97, 2004

[9] 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)

[10] Rezaei. Mehrdad, Jafari. Mahdi, and Amini Lari. Mansour, "Study of routing protocols attacks and security issues in ad hoc network ", First National Conference on Electrical and Computer southern Iran, Islamic Azad University Khormoj, April 2013.(in persian)

[11] CAI. Jiwen, YI. Ping, and CHEN. Jialin, WANG. Zhiyang, and LIU. Ning, " An Adaptive Approach to Detecting Black and Gray Hole Attacks in Ad Hoc Network", 1550-445X/10 $26.00, DOI 10.1109/AINA.2010.143, IEEE, 2010

[12] Yang Su. Ming, " Prevention of selective black hole attacks on mobile ad hoc networks throughintrusion detection systems", Elsevier, 2011

[13] Sergio Marti et al, "Mitigating routing misbehavior in mobile ad-hoc networks," Proceedings of the International Conference on Mobile Computing And Networking ACM (MobiCOM 2000), 2000

[14] Ms. Sonali P. Botkar, Mrs. Shubhangi R. Chaudhary, " An Enhanced Intrusion detection System using Adaptive Acknowledgmentbased, Algorithm", 978-1-4673-0126-8/11/$26.00c 2011 IEEE, IEEE, 2011

[15] 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