**Available Online at www.ijcsmc.com**

**International Journal of Computer Science and Mobile Computing**

**A Monthly Journal of Computer Science and Information Technology**

**ISSN 2320–088X**

*IJCSMC, Vol. 3, Issue. 11, November 2014, pg.570 – 576*

**RESEARCH ARTICLE**

# A Defense Model for Black hole and Gray hole attacks in MANET

**S.V. Vasantha[1], Dr. A. Damodaram[2]**

[1] Associate Professor of CSE Dept., Nishitha College of Engineering and Technology
Greater Hyderabad, India
[2] Professor of CSE Dept., Director AAC, JNTUH, Hyderabad, India
[1] s.v.vasantha@gmail.com; [2] damodarama@rediffmail.com

---

***Abstract--- Mobile Ad hoc Network is one of the most promising technologies in recent years. In MANET, a wireless network is rapidly formed using mobile nodes. Due to its characteristics such as open and undefined medium, dynamic topology, limited resources, lack of centralized control and cooperative environment, providing a secure data transmission in presence of malicious nodes in the network is the major challenge of the MANET. Attacks at the Network Layer such as Black hole and Gray hole exploit one of the MANET routing protocol such as DSR protocol to involve malicious node in the routing process and drop packets. This paper proposes a Defense model for Black hole and Gray hole attacks in the MANET.***

***Keywords--- Mobile Ad hoc Network, Black hole Attack, Gray hole Attack, Security***

---

## I. INTRODUCTION

Mobile Ad hoc Network (MANET) is a type of wireless network in which all nodes are mobile and the network formed with these nodes, change its topology dynamically [1]. Each node in the MANET plays two roles i.e. it acts as a host or end system in the network when it has some data to transmit or receive and it acts as a router to perform networking operations so that the network is formed with these nodes do not require any pre-existing fixed infrastructure and it can be deployed anywhere at any time. It is a multi-hop relay network where mobile nodes that are within the same transmission range can directly communicate whereas mobile nodes which are not in same transmission range cannot communicate directly instead they take help of intermediate mobile nodes to relay their packets. In MANET any mobile node can join or leave the network at any time and they can even change the network topology rapidly because nodes forming the network are movable. In this network, nodes communicate with each other based on the trust among them as there is no central administration to coordinate the communication between them. So, a malicious node can easily enter into the network and become an intermediate node along path

 

thereby gaining the access to the ongoing communication [2]. Due to this dynamic nature and dependence on the intermediate nodes for routing, MANET is exposed to various security attacks.

MANET routing protocols are categorized into proactive, reactive and hybrid. In case of proactive routing protocols each node in the network maintains routes to all other nodes irrespective of their involvement in the data transmission. These protocols not only update routing tables periodically but also update when there is a change in the topology of the network. In contrast, reactive routing protocols do not update routing tables periodically instead they maintain routes when there is a need to find the path to forward packets. Hence they are known as on-demand routing protocols. The reactive routing protocols respond to topological changes in the network. These protocols significantly decrease the routing overhead when the traffic and topological changes are less. Hybrid routing protocols combine proactive and reactive routing mechanisms to find out efficient routes with minimum overhead [3].

In MANET, routing the packets to the destination node is the critical operation of the network because very often the network will arrive with broken links, this is due to intermediate nodes along the path may leave the network frequently or change its transmission characteristics from symmetrical links to asymmetrical links.

Most prominent attacks which exploit MANET weaknesses such as open medium, trusted and cooperative environment and MANET routing protocol weaknesses such as intermediate node relay and routing, are Black hole and Gray hole attacks. Other possible attacks which take advantage of these weaknesses are Worm hole attack, Byzantine attack, Information disclosure attack, Resource consumption attack, Sybil attack and Rushing attack [3][4].

## II. BLACK HOLE AND GRAY HOLE ATTACKS

The Black hole and Gray hole attacks are security attacks which falls under the network layer attacks, they exploit reactive routing protocols of MANET such as DSR, AODV etc., to drop the packets in the network [5]. They take the advantage of cooperative nature of MANET to involve malicious nodes forming the network thereby gaining the legitimate access to the network and carry out Denial of Service (DOS) attack or these malicious nodes drop packets without forwarding to next hop node so that they can save their limited battery power behaving as selfish nodes in the network. The various types of these attacks are Single Black hole attack, Cooperative Black hole attack, Single Gray hole attack and Cooperative Gray hole attack.

### A. Single Black hole Attack

A black hole attack is a security attack where a malicious node uses On-demand routing protocol. When a source node broadcast RREQ packets as a part of route discovery process, malicious node advertises itself as having the shortest path to the destination node with a highest sequence number so that source node selects RREP packet sent by malicious node and it rejects other RREP packets. Once the path through malicious node is selected by the source node which is spurious, it absorb data packets without forwarding them to the next node in the network [6]. Thereby creating a black hole in the network where data packets sent to it are drained. Due to this effect network performance gets down drastically. If this attack is carried out by the single malicious node then it is known as Single Black hole Attack. In Fig. 1 node B is the Black hole node which replies immediately with fresh and shortest path to the RREQ packet flooded by the source node S, but there are valid paths available to the destination node D through intermediate nodes A and E which are not considered.

 

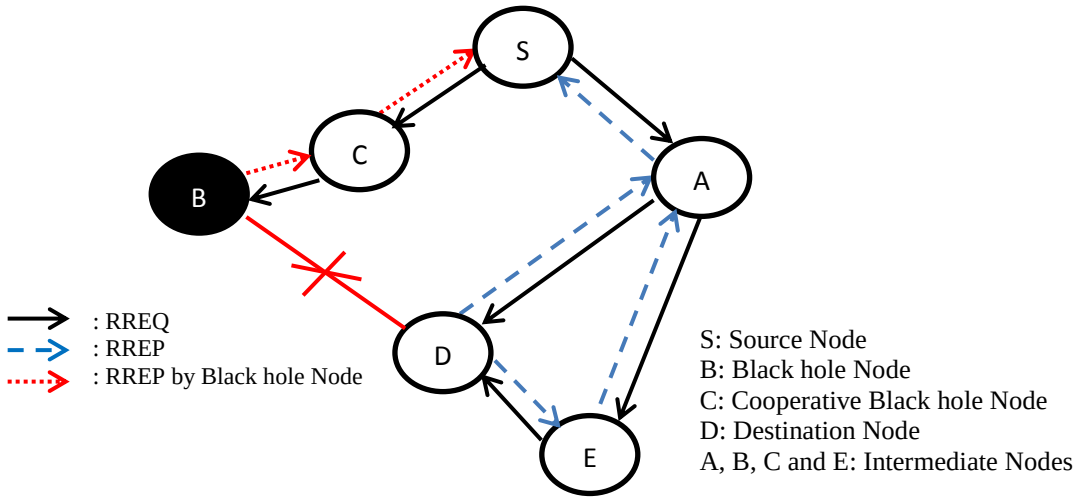


Fig. 1: Black hole Attacks in Mobile Ad hoc Network

B. Cooperative Black hole Attack

The Cooperative Black hole attack is a kind of Black hole attack in which two or more nodes cooperate amongst themselves to form a group [7] and when a source node broadcast RREQ packets into the network, this group of malicious nodes collude and a false RREP packet with shortest and fresh route is sent to source node by them. As soon as source selects this path and forward the data packets, the Black hole node on the path drops these packets without further relay. In Fig.1 node C is the Cooperative Black hole node which helps Black hole node B to carry out the attack. Cooperative Black hole attack is more dangerous than Single Black hole attack because malicious nodes which are nearby form a group and cooperate to escape from the detection process.

C. Single Gray hole Attack

The Gray hole attack is a selective packet dropping attack. In this attack a malicious node becomes a part of route selected by the source node as it replies that it has a valid shortest path. After establishing the spurious route, it forward all packets to certain nodes but drop packets coming from or destined to specific nodes or the node that may behave maliciously for some time but later on it behaves absolutely normally. Due to this uncertainty in behavior of gray hole, this type of attack is more difficult to detect when compared to black hole attack [8]. This attack is also known as Misbehaving attack [9]. If the single malicious node is responsible to accomplish this attack then it is called as Single Gray hole attack. In Fig. 2 node G is the Gray hole node which acts normal for other nodes in the network and drop packets destined to node D or drop packets coming from source node S.

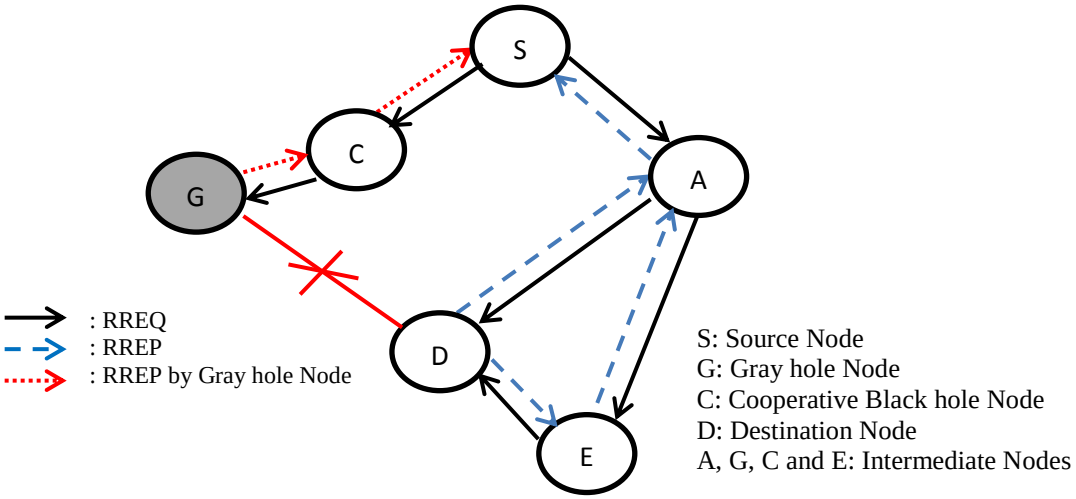


Fig.2: Gray hole Attacks in Mobile Ad hoc Network

 

D. Cooperative Gray hole Attack

Cooperative Gray hole attack is similar to Cooperative Black hole attack but here the nodes which form a group to cooperate and accomplish this attack are Gray hole nodes in place of Black hole nodes. Gray hole itself cannot be identified easily as it toggles its behavior between normal and malicious and if group of them collude to perform an attack then the situation is worst. In Fig.2 node C is the Cooperative Gray hole node which supports the Gray hole node G to perform the attack.

## III. RELATED WORK

Authors in paper [10] presented an algorithm that uses both the concept of cryptographic algorithm RSA and sequence number calculation to eliminate the black hole attack. It provides security for transmitting the packets from source node to destination node. But the method involves computational overhead and it is not addressing the Gray hole attacks.

In paper [11] the authors proposed a mechanism that uses the false RREQ packets to attract the malicious node to respond with the false RREP. In this method, there is more than one malicious node which will reply the false RREQ packet. The RREP packet is improved by adding one more field to indicate the identity of the node which replies with RREP packet. Thus, if any intermediate node sends the RREP message in response to the false RREQ, it can be easily found. The normal nodes will not respond to the false RREQ message as they have no route to that virtual node. The identities of malicious nodes will be added to the black list and this list will be broadcast as an ALARM to all other nodes in the network. So that the multiple black hole nodes will be separated from the network. This mechanism identifies a secure and shortest routing path from a source to a destination in presence of black holes effectively but it is not providing any solution against gray hole attacks.

Gayatri Wahane et al [12] proposed an algorithm for detection of a cooperative black hole attack. It modifies the AODV routing protocol by introducing two concepts i.e. Data routing information (DRI) table and Cross checking. Two additional bits are sent by the nodes that reply to the RREQ message of the source node. Each node maintains an additional data routing information (DRI) table. In the DRI table, the first bit "From" is the information on routing data packet from the node and the second bit "Through" is for information on routing data packet through the node. During Cross checking list of Cooperative Black holes are identified with help of reliable nodes and DRI table entries. The results shows that packet delivery ratio is less than 60% and it cannot address Gray hole attacks.

The mechanism proposed in the paper [13] detects gray hole attacks. It involves both local and cooperative detection to find out any malicious gray hole in the network. As soon as the node is detected to be really malicious, it has a notification mechanism to inform to all the nodes in the network so that the malicious node can be isolated. The mechanism consists of four procedures which are invoked one after the other. They are 1. Neighborhood data collection, 2. Local anomaly detection, 3. Cooperative anomaly detection, and 4. Global alarm raiser. In this scheme the Gray holes are identified with the help of neighbouring nodes. This mechanism do not work if the neighbouring nodes collude to perform Gray hole attack and the results shows that 100% packet delivery ratio is not achieved with this security method.

The paper [14] provides a method for detection of Black hole and Gray hole attacks in MANET when source node wants to send data packets to destination, it demands that the nearby BBN for any restricted IP (RIP). The BBN on obtaining the RIP replies with one of the untouched IP addresses. The source node sends the RREQ packets for both the destination node and the RIP simultaneously. If the source node receive the RREP packet only from the destination node then this the normal case otherwise there is a black hole in that route. In this case source starts the Black hole detection process. It notifies the neighbouring nodes from which it got the RREP to RIP, to enter in to promiscuous mode, so that they observe flow. Source node sends some artificial data packets to the destination node, while the neighbouring nodes start monitoring the packet flow. When the monitoring nodes find that the artificial data packet loss is much more than the standard expected loss in a network, they inform about this malicious node to source. This information is spread throughout the network to list it as black hole. This procedure also works for gray holes as it is detected by any of its neighbouring normal nodes. The limitation of this technique is that it cannot work for Cooperative Gray holes because the method detects malicious nodes based on the information received from the neighbouring nodes.

 

## IV. PROPOSED DEFENSE MODEL

The proposed defense model for Black hole and Gray hole attacks provides the framework for developing a complete solution to combat against the different types of Black hole and Gray hole attacks possible in the MANET. The technique developed using this model not only addresses all these attacks but also provides reliable data transmission in the network. This model considers weaknesses of prominent reactive routing protocols and prevention and/or detection mechanisms for Black hole and Gray hole attacks and provides steps by step procedure to develop a robust solution. The proposed model comprises of four modules which are to be followed when developing the solution. The modules of the model are 1. Adversary Evasion 2. Adversary Recognition 3. Route Maintenance and 4. Data Restoration. Each of these modules is described below.

A. Adversary Evasion

B. Adversary Recognition

C. Route Maintenance

D. Data Restoration

### A. Adversary Evasion

This is the first module of the model in which an elimination mechanism is used to avoid the Black hole and Gray hole nodes from participating in the route discovery process. This is the first line of defense to the system. To prevent the malicious nodes from route discovery process the technique needs to have the knowledge of previous misbehaved nodes with certain rating value indicating its level of severity.

Module 1 Algorithm:

Step 1: Source node checks its route cache for the valid route, if route is available go to step 4 otherwise proceed with next step.

Step 2: Source node broadcast RREQ packets to all nodes in the network.

Step3: Source node collects RREP packets from only destination node and rejects remaining RREPs from intermediate nodes.

Step 4: Check the nodes in RREPs for black listed nodes, if available reject RREPS otherwise proceed to next step

Step 5: If multiple valid routes are available then select one with shortest path and store remaining in the source route cache and go to module 2.

### B. Adversary Recognition

This the second line of defense where a strong detection mechanism is used to find out the malicious node/nodes misbehaving during the data forwarding phase. The detection mechanism to find out the malicious node, it should not depend on the information collected from intermediate nodes adjacent to the malicious node because adjacent nodes collude to carry out a cooperative attack, which is hard to detect. It should confirm the data packet transmission by collecting the information from the destination node only. The detection mechanism requires continuous monitoring of malicious nodes because a gray hole toggles its behavior between honest and malicious. Once the malicious nodes are identified they must be blacklisted so that they will not be allowed to participate during the route discover process in the future.

Therefore a detection mechanism must have two important processes i.e. first process is to identify the malicious nodes and second process is to blacklist the malicious nodes associating a rating value to them so that these rating values can be compared with a threshold value at the time route discovery process and decide whether to allow or reject the nodes in the routing process.

 

Module 2 Algorithm:

Step 1: After selecting the path, send a dummy packet to find black holes if found go to step 3 otherwise proceed

Step 2: Send data packets and check the sequence numbers of ACKs to find any missing ACKs to detect gray holes, if found proceed to next step otherwise go to step 4

Step 3: Black list these malicious nodes and to maintain the route go to module 3.

Step 4: When data transmission is completed i.e. all packets are received then nodes in this route are given good rating.

C. Route Maintenance

This is the next module which involves finding a new path for the remaining data transmission. After detecting the malicious node/nodes on the path, it is informed to the source node. Source node stops sending data packets and checks out its route cache for an alternative path with highest rating value if available otherwise finds a new path by initiating route discovery process. In this route discovery process previously detected malicious nodes are avoided so that the new path found will not contain suspected malicious nodes.

Module 3 Algorithm:

Step 1: Reject the existing path with black listed nodes.

Step 2: Find a new path using module 1 and repeat module 2 step 1 and go to module 4.

D. Data Restoration

The lost data packets are identified by source node with help of the destination node confirmations received. In the case of Black hole attack, source node requires to start the data transmission from the first packet onwards and in the case of Gray hole attack, lost packets need to be identified and resend only the lost packets to the destination node. Next it continues with the remaining data transmission. Thereby all the packets from source node to destination node are transmitted reliably and securely.

Module 4 Algorithm:

Step 1: Corresponding data packets for the missing ACKs are identified and retransmitted.

Step 2: Continue to send remaining data packets and repeat module 2 step 2.

## V. CONCLUSION AND FUTURE WORK

Malicious behavior of the nodes effects network performance severely. Hence providing security in presence of these malicious nodes is the major constraint for deployment of the MANET. In this paper different types of Black hole and Gray hole attacks and various methods proposed to detect and/or prevent these attacks for most prominent routing protocols are discussed. There are various solutions proposed to address Black hole and Gray hole attacks but there is no one complete solution which addresses different varieties of Black hole and Gray hole attacks and provides a reliable, secure and efficient mechanism. The proposed model can be used to develop a technique that gives a complete solution to address these attacks and makes the data transmission reliable. Therefore the future work is to develop and implement a mechanism using this proposed defense model.

 

## REFERENCES

[1] 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 Website: www.ijetae.com (ISSN 2250-2459, Volume 2, Issue 1, January 2012, 37-41)
[2] Mr. Kumar Pradyot Dubey, Er. Kuntal Barua, "A Review - Techniques to Mitigate Black/Gray Hole Attacks in MANET", Engineering Universe for Scientific Research and Management (International Journal), Vol. 6 Issue 6 June 2014, 1-5 Paper ID: 014/EUSRM/6/2014/9046
[3] K.P.Manikandan, Dr.R.Satyaprasad, Dr.K.Rajasekhararao, "A Survey on Attacks and Defense Metrics of Routing Mechanism in Mobile Ad hoc Networks", (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 2, No.3, March 2011 (7-12)
[4] Saloni Sharma , Anuj K Gupta, " Survey of Secure mobile adhoc routing protocols", International Journal of Research in Computer Engineering and Electronics. 1 VOl : 3 ISSUE :2 ISSN 2319-376X ICV 4.08 IJRCEE@2014 http://www.ijrcee.org
[5] Rashmi, Ameeta Seehra, " Detection and Prevention of Black-Hole Attack in MANETS", International Journal of Computer Science Trends and Technology (IJCST) – Volume 2 Issue 4, Jul-Aug 2014, ISSN: 2347-8578 www.ijcstjournal.org Page 204-209
[6] Athira V Panicker, Jisha G, "Network Layer Attacks and Protection in MANET- A Survey", Athira V Panicker et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (3) , 2014, 3437-3443
[7] Jaydip Sen, Sripad Koilakonda, Arijit Ukil, "A Mechanism for Detection of Cooperative Black Hole Attack in Mobile Ad Hoc Networks", IEEE 2011 Second International Conference on Intelligent Systems, Modelling and Simulation, 978-0-7695-4336-9/11
[8] Garima Neekhra, Sharda Patel, Ashok Varma, "A Literature Review on Detection of Gray Hole Attack in MANET AODV Routing Protocol", International Journal of Emerging Technologies and Engineering (IJETE) Volume 1 Issue 7, August 2014, ISSN 2348 – 8050, 186-189
[9] V. Shanmuganathan, Mr.T.Anand, "A Survey on Gray Hole Attack in MANET", IRACST – International Journal of Computer Networks and Wireless Communications (IJCNWC), ISSN: 2250-3501, Vol.2, No6, December 2012, 647-650
[10] G.Vennila, Dr.D.Arivazhagan, N. Manickasankari, "Prevention of Co-operative Black Hole attack in Manet on DSR protocol using Cryptographic Algorithm", G.Vennila et al. / International Journal of Engineering and Technology (IJET), ISSN : 0975-4024 Vol 6 No 5 Oct-Nov 2014 2401-2405
[11] Rohini Sharma, Meenakshi Sharma, "A Technique To Establish Shortest Route In MANET By Detecting Multiple Cooperative Black Hole Attack", Proceedings of IRF International Conference, Bangalore 23rd March-2014, ISBN: 978-93-82702-68-9
[12] Ms. Gayatri Wahane, Prof. Ashok Kanthe, "Technique for Detection of Cooperative Black Hole Attack In MANET", International Conference on Advances in Engineering & Technology – 2014 (ICAET-2014) 59-67
[13] Jaydip Sen, M. Girish Chandra, Harihara S.G., Harish Reddy, P. Balamuralidhar, "A Mechanism for Detection of Gray Hole Attack in Mobile Ad Hoc Networks", 1-4244-0983-7/07/$25.00 ©2007 IEEE ICICS 2007
[14] Vandna Dahiya, Ajay Dureja, "Detection of Black Hole & Gray Hole in MANET", International Journal of Computer Science and Mobile Computing, Vol.3 Issue.7, July- 2014, ISSN 2320–088X, pg. 466-473

 