ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

IJESRT
INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

Black hole and Gray Hole attacks in MANET: A Survey

S.V. Vasantha[*1], **Dr. A. Damodaram**[2]
[*] Associate Professor of CSE Dept., Nishitha College of Engineering and Technology
Greater Hyderabad, India
Professor of CSE Dept., Director AAC, JNTUH, Hyderabad, India

Abstract

Mobile Ad hoc Network is a wireless infrastructure less network formed using mobile nodes. It is a multi-hop relay network where data is forwarded from source to destination using intermediate mobile nodes. If these intermediate mobile nodes are malicious then various security attacks are feasible. Network layer attacks such as Black hole attack, Cooperative Black hole attack, Gray hole attack and Cooperative Gray hole attack are possible in MANET, because MANET routing protocols assume trusted and cooperative environment in the network. This paper discuss about different kinds of Black hole and Gray hole attacks in MANET and their countermeasures.

Keywords- Black hole attack; Gray hole attack; MANET; Security.

Introduction

Wireless networks are fundamentally classified into infrastructure-based networks and infrastructure-less networks. The infrastructure-based networks use fixed access points to coordinate the communication between the mobile nodes. The Mobile Ad hoc Network (MANET) comes under the category of infrastructure-less networks. MANET is self-forming network consisting of mobile nodes, which acts as a router when relaying data for other mobile nodes and acting as a host when transmitting or receiving information to/from other mobile nodes in the network. Therefore the operation of the MANET depends on the cooperation and trust among the mobile nodes forming network.

MANET characteristics such as dynamic topology, open medium, lack of centralized control, limited resources and cooperative environment makes the ad hoc network vulnerable to various security attacks [1]. On the other hand, many of the MANET routing protocols assume that the mobile nodes participating in the routing process are not malicious and work in cooperation but this assumption can be easily compromised by the malicious attackers acting as routers for other mobile nodes and disobeying the routing protocol specifications [2]. Hence various security attacks are possible at network layer.
Few of the significant packet dropping attacks at the network layer which captures the weaknesses of routing protocols are Black hole attack, Cooperative Black hole attack, Gray hole attack and Cooperative Gray hole attack.

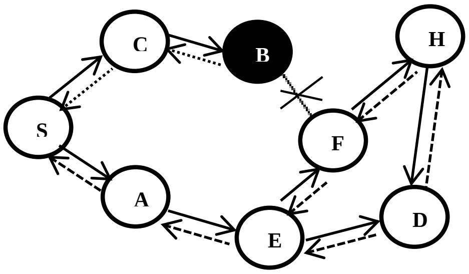
Black hole attack

Black hole attacks are a kind of Denial Of Service (DOS) attacks [3] because packets are not forwarded to the destination mobile node instead dropped by the Black hole nodes in the network. Black hole attack comprises of two phases [4].

In first phase of the attack the malicious node exploits the MANET reactive routing protocol such as DSR. During the route discovery process source node floods RREQ packets into the network to find a path from source node to the destination node. As soon as RREQ packet is received by the malicious node, it replies with false RREP containing a fresh valid shortest path immediately without checking its route cache [5]. When source node receives multiple RREPs, it selects the RREP with highest sequence number and discards the other RREPs thereby a malicious node becomes an active router for relaying the packets of source node.

In second phase of the attack, once malicious node is included in the selected route from source node to destination node, packets forwarded to it are dropped without forwarding to the next hop. Hence the malicious node behaves like a black hole absorbing packets on the path.

An example of Black hole attack is shown in the fig. 1. When source node S has some data to transmit it starts the route discovery process by flooding RREQ packet into network, then immediately Black hole node B responds with a spurious route without checking its route cache. Source node S receives three replies; one is from the black hole node B, which specifies fresh and shortest path and other two paths (S-A-E-D and S-A-E-F-H-D) are replied from any intermediate node or destination node D. Eventhough there is a valid shortest path S-A-E-D exists between Source node S and destination node D, Source node S selects the Black hole node's reply because it is fresh and shortest path than all other replies. On the selected path source node S starts sending data packets but these packets are not received by the destination node D because Black hole node B in the path drops the packets without forwarding it to next hop node F.



S: Source Node
B: Black hole Node
D: Destination Node
A, B, C, E, F and H: Intermediate Nodes

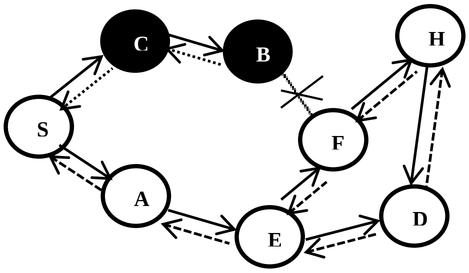
⟶ : RREQ
- - -> : RREP
·····> : RREP by Black hole Node

Fig. 1. Black hole attack scenario

Cooperative black hole attack

If malicious node participating in the Black hole attack is only one then it is known as single Black hole attack otherwise if malicious nodes in the attack are two or more then it is known as Cooperative Black hole attack. In this attack group of malicious nodes cooperate among themselves to carry out the attack. When the packet is forwarded to any of these malicious nodes then they collude with each other to drop it.

Cooperative Black hole attack is depicted in the fig. 2. Here the nodes B and C are colluded to perform the attack. Basically the Black hole detection schemes detect Black hole based on the information received from the neighbouring nodes [6][7], this weakness can be exploited by the cooperating Black hole nodes. In this example node C, which is significant to detect Black hole node B is compromised and cooperating with it. Hence making single black hole node detection scheme not suitable for detecting Cooperative Black hole nodes in the network.



S: Source Node
Band C: Cooperative Black hole Nodes
D: Destination Node
A, B, C, E, F and H: Intermediate Nodes

⟶ : RREQ
- - -> : RREP
·····> : RREP by Black hole Node

Fig. 2. Cooperative Black hole attack scenario

Gray hole attack

Gray hole attack is a variant of black hole attack in which a malicious node switches its behaviour between honest to malicious. During route discovery process a gray hole node behaves as a honest node, once it is included in the path it switches its behaviour into malicious node and drops some or all the packets sent to it without forwarding to the next hop in the network [8]. It may drop packets coming from a particular mobile node or destined to a particular mobile node and behaves like a trusted node forwarding all the packets for other mobile nodes in the network. It may behave as a honest node for a certain time period and suddenly changes its behaviour into a malicious node dropping the packets without forwarding into the next hop. Due to this unpredictable behaviour of the gray hole node it is hard to detect them when compared to black hole node. In this attack, packets are dropped with a certain probability [9].

Gray magnitude of a gray hole node specifies the percentage of the packets dropped by it without further relaying to next hop [10].

Gray hole attack example is shown in the fig. 3. In this example, gray hole node G is silent during the route discovery process and later at the time of data forwarding it switches its behavior from honest to malicious, thereby dropping the packets sent to it without forwarding to the next hop F. After some time again it may switch its behavior back to honest forwarding the packets so that it is not detected by the detection mechanisms.

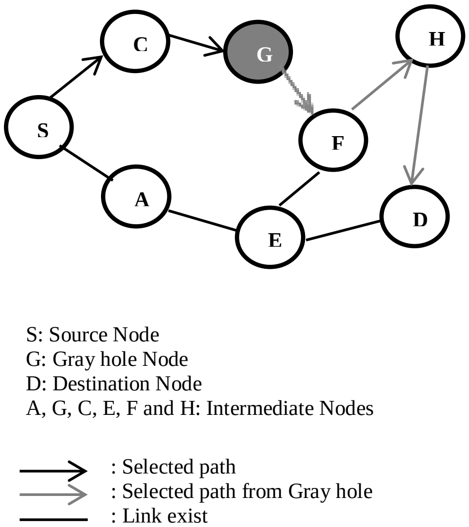


Fig. 3. Gray hole attack scenario

Cooperative gray hole attack

Cooperative Gray hole attack is similar to Cooperative Black hole attack, where a group is formed with two or more mobile nodes which cooperate among themselves to go malicious activity undetected from the detection process. Detecting a Gray hole attack is difficult because of its unpredictable nature and if group of malicious nodes collude to carry out this attack then it is more difficult to detect them.

Related work

N. Bhalaji et al [11] proposed a Trust based model to mitigate Black hole attacks in DSR protocol, which is based on the association among the nodes. It chooses the most reliable and secure route to the destination node based on the trust values of nodes. For every node in the network, a trust value is computed and stored that represent the value of the trustiness to each of its neighboring nodes. Later these trust values are adjusted based on the experiences of the node with its neighboring nodes. Limitations of this technique are, it does not address Gray hole and Cooperative Gray hole attacks.

P. Subathra et al [12] proposed a technique for detecting Single and Cooperative Black hole nodes in mobile ad Hoc network, based on distributed probing scheme. This scheme uses an alternate path to detect the presence of malicious nodes by probing and observing the acknowledgments. Drawback of this technique is gray hole nodes are left undetected.

In paper [13] a watch dog and path rater based approach was proposed by the authors to identify and exclude malicious nodes in MANET. Each node acts as a watch dog for the next node to check its forwarding (goodness) nature using an implicit acknowledgment technique. Limitation of this approach is that it cannot detect malicious nodes in presence of ambiguous collisions or limited transmission power.

In paper [14] authors proposed an explicit acknowledgment based approach for detecting misbehaving nodes in MANETs. Two- hop Acknowledgments are sent in opposite direction of the path to monitor next hop's forwarding nature. Limitations of this mechanism are it increases overhead and cannot handle cooperative attacks.

In paper [15] a modified DSR for mitigating Black hole Impact in MANET was proposed. In this approach a source node uses RREP available in its route cache or sent by an intermediate node for forwarding the first data packet and waits for the acknowledgment (ack). If ack comes within a certain time, then this route is safe and succeeding packets are sent on the same route otherwise to identify the presence of malicious node a fictive route request is sent along the suspected route with the destination address as fictive address which is not there in the network.

The node that replies to this fictive route request is listed as black hole and it is not included in the further routing process. If the route reply is from destination node then the route is considered as safe route. Limitations are it does not address Gray Hole attacks and Cooperative Gray hole attacks.

Authors in paper [16] proposed a novel Gray hole attack detection mechanism for MANET, which has three related algorithms. First algorithm is the Creating Proof Algorithm, where each node involved in the routing process i.e. source node and intermediate nodes must create a proof based on aggregate signature algorithm to prove that it has received a message.

Second algorithm is the checkup algorithm, when there is a suspect that the packets are being dropped in the network then this algorithm is called to identify the malicious nodes in the network. Third algorithm is the diagnosis algorithm. In this algorithm according to the received proofs, the source node might trace the malicious node. This algorithm limits to Gray holes detection.

Arti Tiwari et al [17] proposed a mechanism for detection of Black hole and Gray hole attacks in mobile ad hoc network for AODV routing protocol using Zero knowledge Protocol (ZKP) and Extended Data routing Information (EDRI) table. It uses ZKP technique to prevent the network from repudiation attack and EDRI Table for detection of Black hole and Gray hole nodes in the network. In the EDRI table a counter is maintained to record the packet dropping nature of the malicious nodes and if this malicious behavior is frequently repeated over time then for that node next chance is not given thereby detecting Black hole and Gray Hole nodes in the network. Limitation of this mechanism is the overhead involved which increases the latency thereby degrading the performance of the network.

Conclusion

In this paper different kinds of Black hole and Gray hole attacks are discussed in detail. There are various mechanisms proposed to address these attacks but there is no single technique which provides secure, reliable and efficient data transmission against all these possible Black hole and Gray hole attacks in the mobile ad hoc network. A Mechanism can be proposed to develop a technique that gives a complete solution to address these attacks and makes the data transmission reliable with minimum time delay and maximum packet delivery ratio.

References

1. Kamal Kumar Chauhan, Amit Kumar Singh Sanger, Virendra Singh Kushwah, " Securing On-Demand Source Routing in MANETs", IEEE Second International Conference on Computer and Network Technology, 978-0-7695-4042-9/10.
2. Nan Kang, Elhadi M. Shakshuki, Tarek R. Sheltami, "Detecting Forged Acknowledgements in MANETs", IEEE 2011 1550-445X/11 DOI 10.1109/AINA.2011.84.
3. Dinesh Mishra, Yogendra Kumar Jain, Sudhir Agrawal, "Behavior Analysis of Malicious Node in the Different Routing Algorithms in Mobile Ad Hoc Network", IEEE 2009 International Conference on Advances in Computing, Control, and Telecommunication Technologies, 978-0-7695-3915-7/09
4. 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
5. Reza Amiri, Marjan Kuchaki Rafsanjani and Ehsan Khosravi, " Black Hole Attacks Detection by Invalid IP Addresses in Mobile Ad Hoc Networks", Indian Journal of Science and Technology, Vol 7(4), 401–408, April 2014
6. Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, and Yoshiaki Nemoto "Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method". International Journal of Network Security, Vol.5, No.3, PP.338–346, Nov. 2007
7. Hongmei Deng, Wei Li, and Dharma P. Agrawal, "Routing Security in Wireless Ad Hoc Network," *IEEE Communications Magazines, vol. 40, no. 10, October 2002*.
8. Shalini Jain, Mohit Jain, Himanshu Kandwal, "Advanced Algorithm for Detection and Prevention of Cooperative Black and Gray Hole Attacks in Mobile Ad Hoc", 2010 International Journal of Computer Applications (0975 – 8887)Volume 1 – No. 7.
9. 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 ", IEEE ICICS 2007, 1-4244-0983-7/07
10. Jiwen CAI, Ping YI, Jialin CHEN, Zhiyang WANG, Ning LIU, "An Adaptive Approach

to Detecting Black and Gray Hole Attacks in Ad Hoc Network", 2010 24th IEEE International Conference on Advanced Information Networking and Applications 1550-445X/10 AINA.2010.143.

11. N. Bhalaji, A. Shanmugam, "A Trust Based Model to Mitigate Black Hole Attacks in DSR Based Manet", European Journal of Scientific Research ISSN 1450-216X Vol.50 No.1 (2011), pp.6-15
12. P. Subathra,S. Sivagurunathan, N.Ramaraj, "Detection and Prevention of Single and Cooperative Black Hole Attacks in Mobile Ad hoc Networks ", Intenational Journal of Business Data Communications and Networking,6(1), 38-57, January-March 2010
13. Sergio Marti,T.j., Giuli,K.L., & Baker, M.(2000).Mitigating routing misbehavior in mobile ad hoc networks. In Procreedings of the 6th Annual International Conference on Mobile Computing and Networking, pp.255-265.
14. Liu, K., Deng, J., Varshney, P. K., & Balakrishnan, K.(2007). An acknowledgement based approach for the detection of routing misbehavior in MANNETs. IEEE Transactions on Mobile Computing, 6(5), 536-550. doi:10.1109/TMC.2007.1036
15. Vaishali B. Mewada, Viral Borisagar, " MODIFIED DSR FOR MITIGATING BLACKHOLE IMPACT IN MANET", International Journal For Technological Research In Engineering Volume 1, Issue 9, May-2014 ISSN (Online): 2347 - 4718 www.ijtre.com
16. Gao Xiaopeng Chen Wei, "A Novel Gray Hole Attack Detection Scheme for Mobile Ad-Hoc Networks", IEEE 2007 IFIP International Conference on Network and Parallel Computing – Workshops, 0-7695-2943-7/07
17. Arti Tiwari, Prof. Nilmani Verma" A Novel Scheme for Intrusion Detection & Anticipation of Black Hole & Gray Hole Attacks In AODV Based MANET using ZED", International Journal Of Engineering And Computer Science ISSN:2319-7242 Volume 3 Issue 5, May 2014, Page No. 5744-5751