02- Days, International Conference on Recent Trends in Engineering Science, Humanities and Management
Sri S Ramasamy Naidu Memorial College, Sattur, Tamil Nadu, India (RTESHM-17)
02nd-03rd February 2017, www.conferenceworld.in ISBN: 978-93-86171-18-4

IMPACT OF BLACK HOLE ATTACKS IN MANET - A STUDY

Ranichitra.A[1], Mallairaj. A[2]

[1]Assistant Professor, Department of Computer Science, Sri S.R.N.M College,Sattur, (India)

[2]M.Phil Scholar, Department of Computer Science, Sri S.R.N.M College, (India)

ABSTRACT

Mobile Ad hoc Network (MANET) is an emerging technology which is an autonomous collection of wireless mobile nodes that are self configured to form a network environment without any infrastructure establishment. MANET can form a spontaneous network either momentarily or permanently. The network topology of MANET may often change rapidly and it is not predictable. The decision-making with respect to route is autonomous by the nodes themselves. Due to its unique features like dynamic topology, self–organising and frequent link failure, MANET is susceptible to various attacks. MANET has to be secured against the various security threats. In this paper, black hole attack which is a serious attack in the network layer is discussed. In black hole attack, a malicious node advertises itself as it having the optimal route to the destination, so that all packets will be transmitted through it. This paper discuss the various techniques that have been proposed for black hole attack detection and removal methods.

Keywords— MANET, Black Hole Attack, Security Layers, Protocols.

I. INTRODUCTION

Mobile Ad hoc Network (MANET) can form a spontaneous network at will momentarily. The information transmitted by a mobile node will be received by all the other nodes within its transmission range due to its wireless connectivity and omni-directional antenna based on predefined protocol.

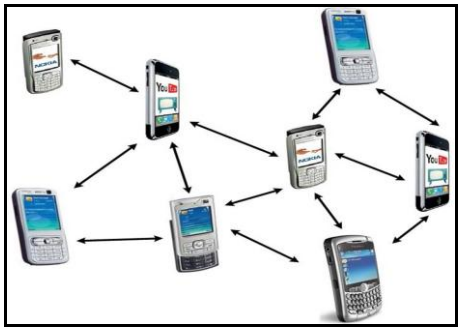

Figure 1 Mobile Ad hoc Networks

Thus each node in the network can act both as a mobile node and as a router to forward the packets in communication area. Due to the limited transmission capability of the network, the nodes cannot directly

ISBN: 978-93-86171-18-4

communicate with those which are not one-hop neighbours. This weakness is overcome through multi hop-communication. They transmit the packets to the other nodes across the network without any access points and any infrastructure establishment. Every mobile node in a network is autonomous as shown in figure 1.

The mobile devices are free to move haphazardly and organize themselves arbitrarily. The Nodes in the MANET share the wireless medium and the topology of the network changes erratically and dynamically. In MANET, breaking of communication link is very frequent, as nodes are free to move anywhere. Routing protocol is used to establish the route from source to destination and to forward the packets between the nodes. The routing protocols can be classified as Reactive routing protocol, Proactive routing protocol and hybrid routing protocol.

In reactive routing protocol, is established the route only when it is needed. To discover a new route reactive protocol makes use of route request and route reply messages. After receiving route reply messages the route is established by the nodes. Route discovery makes a big delay and it is the major drawback of this protocols. In proactive routing protocol the route table constantly maintains the network topology. In the network every node contains the information about the neighbors. This information is stored in different tables and these tables are updated when the network topology changes. Hybrid routing protocol is a combination of proactive and reactive protocols. These protocols make use of distance vector as more precise metrics to establish the best paths to destination networks. Source initiates the establishment of route to the given destination on demand during reactive operation [1]. In MANET, all networking functions such as routing and packet forwarding, are performed by nodes themselves in a self-organized manner. Due to these unique features, securing a mobile ad hoc network is very challenging.

1.1 Attacks In Manet

Secure communication in MANET is important for secure transmission of information. Absence of the central co-ordination mechanism and shared wireless medium makes MANET more vulnerable to digital/cyber attacks than wired network. Table 1 summarizes the MANET security layers and attacks.

Table 1 MANET Security Layers and Attacks.

MANET Security Layer	Attacks
Application Layer	Malicious code, Repudiation
Transport Layer	Session hijacking, SYN Flooding
Network Layer	Flooding, Black Hole, Grey Hole, Worm Hole, Link Spoofing etc.
Data Link Layer	Traffic analysis and monitoring.
Physical Layer	Traffic Jamming, Eavesdropping

The attacks can be classified as passive attack and active attack as shown in figure 2.

ISBN: 978-93-86171-18-4

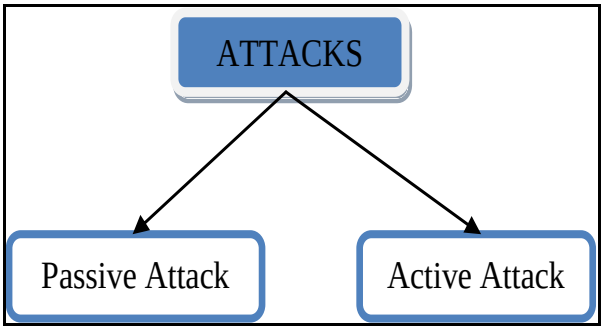

Figure 2 Types of attack

1.1.1 Passive attack:

In this type of attack, the intruder monitors on certain connections to get information about the traffic without injecting any fake information [2]. This type of attack serves the attacker to gain information and makes the footprint of the invaded network in order to apply the attack successfully. Some of the passive attacks are eavesdropping, traffic analysis and snooping.

1.1.2 Active attack:

An active attack attempts to adjust or destroy the data being exchanged in the network, thereby disrupting the functioning of the network. It can be classify into two categories external attacks and internal attacks. External attacks are carried out by nodes that do not belong to the network. These attacks can be prevented by using standard security mechanisms such as encryption techniques and firewalls. Internal attacks are carried out by compromised nodes that are really a part of the network. Since the attackers are already a part of the network as authorized nodes, internal attacks are harsher and not easy to detect when compared to external attacks [3]. The types of Active attacks are wormhole attack, black hole attack, byzantine attack, Sybil attack, gray hole attack. In this paper, black hole attack is considered for the study.

The rest of the paper is organized as follows. Section II, present the literature survey and the comparison of various black hole attack. Section III, discusses the black hole attack in MANET. In section IV, discusses the various black hole attack detection and removal methods and the paper is concluded in Section V.

II. RELATED WORK

Sathis et al [3] proposed a novel strategy to reduce single and collaborative black hole attack. In the proposed method fabricated RREQ and next hop information for mitigating both single and collaborative black hole attack has been generated based on the destination sequence number. The black hole node is identified and black hole list is generated. The proposed method is used the digital signature and trust value to identified the black hole in MANET. The method shows 70% decrease in end-to-end delay, 12% increase in throughput 40% increase in Packet Delivery Ratio.

Nidhi choudhary et al [4] proposed a new solution against the black hole attack to demonstrate a timer based detection approach for identifying black hole node. In this approach initially each node in the network assigns a maximum trust value to all its neighbouring nodes to detect and remove the black hole nodes from the network during the communication process. . To solve this problem, a timer based detection approach is used to detect the black hole attack, to improve the performance of the communication by removing the black hole attack.

ISBN: 978-93-86171-18-4

Kumar singh et al [5] proposed a novel strategy to identify promiscuous mode and to detect the malicious (black hole) node to propagate the information malicious node to all the other nodes in the network. This mode allows a node to intercept and read each network packet that arrives to it. The proposed method uses promiscuous mode of a node to overhear the neighbour's communication. It does not require any database, extra memory and more processing power.

Sakshi jain et al [6] proposed a novel strategy to deploy the base node in the network that increases the probability of detecting multiple malicious nodes. The proposed method exploit the fact that black hole node send route reply to every route request it receive whether it has route to destination or not. This method greatly reduces the probability of black hole attack in network and detects multiple black hole nodes in a network. This approach help in detecting black hole attack in network with the help of bogus RREQ, results has been analyzed with the help of Packet Delivery Ratio, throughput and delay metrics.

Junhai Luo et al [7] proposed a novel strategy which addresses the black hole problem using an authentication mechanism, based on the hash function. The message authentication code and pseudo random function is proposed prevent the black hole attack. [7] Proposed an authentication mechanism for identifying exploited by malicious node. This mechanism is used to handle unlimited message authentication by switching one-way-hash chains and to prevent a malicious node in forging a reply. The simulation results show that the scheme provides fast message verification identifying the black hole and discovers the safe routing.

Jain-Ming chang et al [8] proposed a method to resolve the collaborative black hole attack using DSR routing mechanism, which is referred as the Cooperative Bait Detection Scheme. The proposed collaborative black hole attack detection scheme aims at detect and prevent the malicious nodes by launching collaborative black hole attacks in MANET. The simulation results revealed that the CBDS outperforms DSR In terms of routing overhead and Packet Delivery Ratio.

Akanksha Jain [9] proposed a method trust based communication in MANET using AOMDV-IDS against the black hole attack. AOMDV-IDS perform real time detection of attacks using AOMDV routing protocol. In AOMDV, RREQ transmission from the source to the target establishes multiple reverse paths both at intermediary nodes in addition to the destination. Multiple RREPs navigates this reverse route back to from multiple onward routes to the target at the source and intermediate nodes. Multiple routes revealed are loop-free and disjoint. AOMDV depends on the routing information previously available in the AODV protocol, thus preventing the overhead acquired in determining multiple paths.

Ankur mishra et al [10] proposed a mechanism to mitigate single black hole attack as well as cooperative black hole attack to discover a safe route to the destination. The scheme of proposed approach is based on AODV protocol which is improved by deploying advanced Date Routing Information table with additional check bits. The proposed security mechanism consist of Neighborhood data collection and local malicious node detection, finding trusted node to destination and complete elimination of cooperation black hole nodes, establishing secure path to destination and global alarm arising and blacklisting malicious nodes. The proposed solution can be applied to identify multiple black hole nodes cooperating with each path from source to destination. This method shows the effect of Packet Delivery Ratio and throughput with respect to the variable node mobility.

ISBN: 978-93-86171-18-4

III. BLACK HOLE ATTACKS

Black hole attack is a kind of active attack. In this attack, Black hole waits for neighbouring nodes to send RREQ messages. On receiving an RREQ message, without checking its routing table, immediately sends a false RREP message giving a route to destination over itself, and set a high sequence number to make entry in the routing table of the victim node. Therefore requesting nodes assumes that the route discovery process is completed and ignores other RREP messages and begins to send the packets through the malicious node. Hence in black hole attacks, all RREQ messages are routed through the compromised node, which will not be forwarded anywhere. They are two types of black hole attack.

Single Black Hole Attack:

In a single black hole attack, single node is involved in the attack. A sample scenario of single black hole attack is shown in Figure 3. The malicious node replies to RREQ packets with RREP packets as it is having the shortest path to the destination. And the source node updates the route table and avoids other nodes RREPs since the malicious node has advertised the shortest path. Further the malicious nodes will drop the packets without forwarding the packets to its neighbors.

In this scenario, the node 1 is source node, node 6 is the destination node and node 3 is assumed as the malicious node. When node 1 wants to send the data packets to node 6, it starts the route discovery process by broadcasting RREQ message to the neighboring nodes. So, the nodes 2, 4 and 5 will receive RREQ message. Since node 3 is a malicious node. It immediately sends a RREP message to node 1 with high sequence number and node 1 assumes that it is the freshest route and ignores all other RREPs and sends the packets to the destination. However the node 3 drops all packets instead of sending the packets to the intended destination.

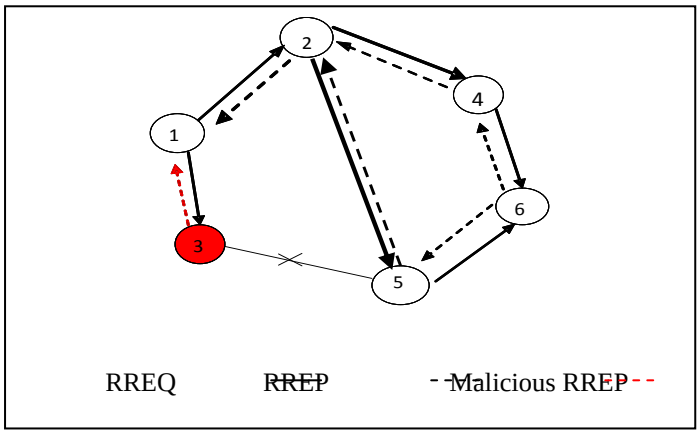

Figure 3, Single black hole attack

Collaborative black hole attack

In collaborative black hole attack, more than one node will involve in this attack and aims to disturb the normal functioning of the network. These malicious nodes claim itself of being the shortest path to the destination and drop the routing packets without forwarding to its neighbors. A sample scenario of collaborative black hole attack is shown in Figure 4.

ISBN: 978-93-86171-18-4

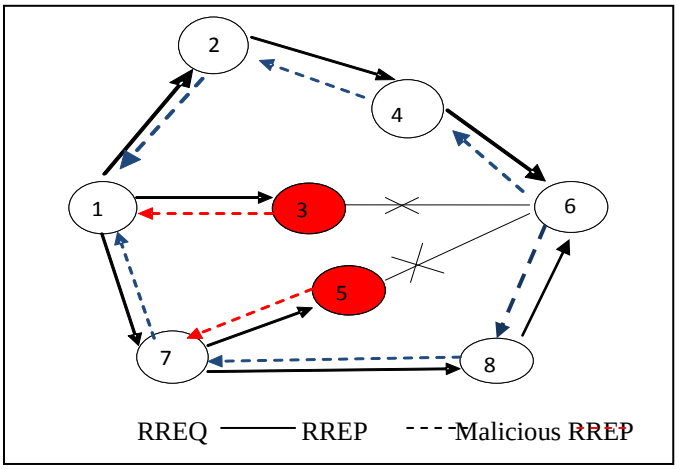

Figure 4 Collaborative black hole attack

In this scenario, the node 1 is source node, node 6 is the destination node and nodes 3, 5 are assumed as the malicious node. When node 1 wants to send the data packets to node 6, it starts the route discovery process by broadcasting RREQ message to the neighboring nodes. So, the nodes 2, 4,7and 8 will receive RREQ message. Since node 3 and node 8 is a malicious node, it immediately sends the RREP message to node 1 with high sequence number and node 1 assumes that it is the freshest route and ignores all other RREPs and sends packets to the destination. However the node 3 and node 8 drops all packets instead of sending the packets to the intended destination. Table 2 summarizes the various black hole detection and removal methods with its advantages and disadvantages.

Table 2 Summary of various black hole detection and removal methods

S No	Method	Type of black hole	Methodology	Advantages	Disadvantages
1	Watchdog Method [11]	Single black hole	Malicious node can be detected.	As it is a simplest method, one node only monitors its next node in the route.	There is no predefined limit to differentiate malicious nodes and increase the no. of mistakes to find black hole attack.
2	Strong Node Method [12]	Single black hole	Is an additional node, which help source and destination to find black hole attack	Strong nodes decrease the no. of monitoring of neighbors, only node in particular area of malicious node start monitoring.	This method assumes that strong nodes are trustable, but there is no solution given for attacks.
3	DRI Method [13][14]	Cooperative black hole	This method used for Data Routing Information table.	This method can find any cooperative black hole attack.	These methods works very slowly if there is not any attack in the network and generate huge overhead for checking all nodes in an area.

ISBN: 978-93-86171-18-4

4	SCAN Method [15]	Cooperative black hole	Used two ideas to protect AODV in MANET they are local collaborative and information cross validation.	Each node uses a token which authenticates the node to the entire network.	If there is no neighbor in the network that can cross-checks the route, this method fails.
5	R-AODV Method [16]	Single black hole	Reliable-AODV improves route discovery process of AODV protocol and prevents black hole and gray hole nodes.	It helps to isolate multiple black hole and gray hole nodes.	It increases routing overhead by forwarding RREP after detection of misbehavior.
6	MR-AODV Method [17]	Single black hole	Modified Reliable-AODV used to detect and isolate multiple black hole and gray hole nodes.	MR-AODV isolate black hole and gray hole node during route discovery phase as R-AODV and sets up a secure route for data transmission.	MR-AODV attempts to reduce routing overhead by not forwarding RREP after detection of misbehavior.
7	IDAD Method [18]	Multiple black nodes	A solution based on Intrusion Detection using Anomaly Detection to prevent both single and multiple black hole nodes.	To avoid false positive alarms of intrusion detection. This technique checks multiple anomaly condition.	Neighbor nodes may give false.

V. CONCLUSION

Black hole attack is a serious active attack in MANET. In black hole attack, a malicious node advertises itself as it is having the optimal route to the destination. In this paper the various techniques used for detecting the black hole attacks in MANET is discussed and compared. The detection techniques which uses reactive routing protocols have low overheads, but have high packet loss, it can be concluded the black hole attacks degrades the performance of the network. In the future a suitable solution to detect the black hole attack has to be proposed in such a way that the packet loss will be minimum.

REFERENCES

[1]. Mehul Vasava, 2Mr. Hardik Patel "*Comparison of Different Methods for Gray Hole Attacks on AODV based MANET*" © 2014 IJEDR | *Volume 2, Issue 1* | *ISSN: 2321-9939.*

[2].Maha Abdelhaq, Rosilah Hassan, Mahamod Ismail, Raed Alsaqour, Daud Israf, "*Detecting Sleep Deprivation Attack over MANET Using a Danger Theory –Based Algorithm*", International Journal on New Computer Architectures and Their Applications (IJNCAA) 1(3): 534-541 The Society of Digital Information and Wireless Communications, 2011 *(ISSN: 2220-9085).*

 ISBN: 978-93-86171-18-4

[3]. Sathish M, Arumugam K, S.Neelavathy Pari Harikrishnan V S "*Detection of Single and Collaborative Black Hole Attack in MANET*" *978-1-4673-9338-6/16/ IEEE* WiSPNET 2016 conference.

[4]. Nidhi Choudhary, Dr.Lokesh Tharani "*Preventing Black Hole Attack in AODV using Timer-Based Detection Mechanism*" SPACES-2015, Dept of ECE, K L UNIVERSITY.

[5]. Kumar Singh, Govind Sharma "*An Efficient Prevention of Black Hole Problem in AODV Routing Protocol in MANET*" 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications *978-0-7695-4745-9/12 © 2012 IEEE.*

[6]. Sakshi Jain, Dr. Ajay Khuteta "*Detecting and Overcoming Blackhole Attack in Mobile Adhoc Network*" *978-1-4673-7910-6/15/ 2015 IEEE.*

[7]. Junhai Luo, Mingyu Fan, and Danxia Ye "*Black Hole Attack Prevention Based on Authentication Mechanism*" *1-4244-2424-5/08/ ©2008 IEEE.*

[8]. Jian-Ming Chang, Po-Chun Tsou, Isaac Woungang "*Defending Against Collaborative Attacks by Malicious Nodes in MANETs: A Cooperative Bait Detection Approach*" IEEE SYSTEMS JOURNAL, *VOL. 9, NO. 1, MARCH 2015.*

[9]. Akanksha Jain, "*Trust Based Routing Mechanism Against Black Hole Attack using AOMODV-IDS System In MANET Format*" IJETAE, *vol. 2, April 2012.*

[10]. Ankur mishra, Ranjeet Jaiswal, Sanjay Sharma "*A Novel Approach for Detecting and Eliminating Cooperative Black Hole Attack using Advanced DRI Table in Ad hoc Network*" *978-1-4673-4529-3/12/ 2012 IEEE.*

[11]. Viswa Jhananie K.R, *"An Efficient Algorithm for Detecting and Removing Black hole Attack for Secure Routing in Mobile Ad-hoc Network"* International Journal of Applied Engineering Research ISSN 0973-4562 Volume 11, Number 5 (2016) pp 3186-3191.

[12]. Agrawal, P., Ghosh, R. K., and Das, S. K. 2008. "*Cooperative black and gray hole attacks in mobile adhoc networks*". In Proceedings of the 2nd International Conference on Ubiquitous Information Management and Communication, Suwon, Korea, 310-314.

[13]. Ramaswamy, S., Fu, H., Sreekantaradhya, M., Dixon, j., and Nygard, K. 2003. "*Prevention of cooperative black hole attack in wireless ad hoc networks*". In Proceedings of the International Conference on Wireless Networks.

[14]. Biswas, K., and Liakat Ali, M. D. 2007 "*Security Threats in Mobile Ad Hoc Network*". Master Thesis.Thesis no: MCS-2007:07. , Blekinge Institute of Technology.

[15]. Yang, H., Shu, J., Meng, X., and Lu, S. 2006. *SCAN: "Self-organized network-layer security in mobile* ad hoc networks", J. IEEE Selected Areas in Comm. Vol. 24, No. 2 (Feb. 2006), 261-273.

[16]. RUTVIJ H. JHAVERI, SANKITA J. PATEL, DEVESH C. JINWALA, "*Improving Route Discovery for AODV to Prevent Black hole and Grayhole Attacks in MANETs*", INFOCOMP, v. 11, no. 1, p. 01-12,March-2012.

[17]. Rutvij H. Jhaveri, "*MR-AODV : A solution to mitigate blackhoe and grayhole attacks in AODV based MANETs*".

[18]. Varsha Patidar, Rakesh Verma "Black Hole Attack and its Counter Measures in AODV Routing Protocol" *International Journal Of Computational Engineering Research (ijceronline.com) Vol. 2 Issue. 5.*