Survey of Malicious Attacks in MANET

Neha Shrivastava
M. Tech. (CSE)
NRI Institute of Research &
Technology Bhopal, India.

Anand Motwani
Assistant Professor (CSE)
NRI Institute of Research &
Technology Bhopal, India,

ABSTRACT

A Mobile Ad hoc Network (MANET) is a collection of mobile nodes and is autonomous having communication through the insecure wireless links. The nodes in the network dynamically add and join the network. Due to this kind of nature nodes are vulnerable to various kinds of attacks. There are many threats in wireless Mobile Ad hoc Networks. MANETs suffers from intrusion in which a malicious node may or may not participate in route discovery mechanism with an intension to degrade the overall network performance. Intrusion has serious impact on routing and delivery ratio of packets. Many researchers have conducted different techniques to propose different types of detection and prevention schemes. Here various attacks types and a survey of the existing solutions is presented.

Keywords

Mobile Ad hoc Network, MANET, Security, Black hole attack, Gray hole attack, Worm hole attack.

1. INTRODUCTION

MANET is a wireless network formed by collection of mobile nodes without the preset infrastructure. When network topology changes nodes in range still remains connected. The major shortcoming is their limited bandwidth, memory, processing capabilities and open medium and so these are more prone to malicious attacks [8]. Due to its dynamic topology and no infrastructure in wireless ad-hoc networks they are exposed to lot of attacks. MANET is well known for its properties. It is flexible and maintains the connectivity between devices when a node moves from one location to another. Another property is neighbor and route discovery so that the data can be routed from source node to neighboring node till it reaches to the destination. When a new network is to be established then it requires only new set of nodes with limited wireless communication range.

Though it has a wide usage there are several open issues about MANETs, such as security threats, finite bandwidth, malicious broadcasting messages, reliable data delivery, dynamic path establishment and limited hardware. The security threats have been discussed and investigated in the wired and wireless networks [14]. Challenges that need to be considered prominently are: Firstly, difficult to implement security mechanisms. Secondly: limited power and resource availability. The researchers mainly focused on establishing the shortest and secure route for the data packets in a dynamic changing environment with minimum cost of bandwidth and battery power [15].

Routing protocols are principally a standard that decide the behavior of the node in context to route the data packet from one node to another. Routing protocols can be classified as Link State protocol and Distance Vector Protocol. Link State protocols build the topology of the entire network for calculating routes and then calculate the best path. These protocols consume more power and memory resources.DSR and OLSR are examples of such protocols. While in Distance Vector protocols router keeps information of their neighbors only and calculate the cost based on it. AODV is one of the Distance Vector routing protocol.

Based on another classification Routing protocols are of three types: Proactive, Reactive and Hybrid. In Proactive routing protocol each node maintains routing table periodically and therefore also known as table driven protocol. OLSR is one of the examples of it. In Reactive routing protocol route is only determined when it is required and therefore it is also known as On-Demand routing protocol. AODV and DSR are examples of it. Hybrid routing protocol as name suggests is a combination of Proactive and Reactive routing. Initially proactive routing is used to gather the unfamiliar routing information and then the reactive routing is used to maintain the information when network topology changes. Zone Routing Protocol (ZRP) is one of the hybrid protocols.

In the rest of the paper, Section 2 briefly introduces classification and definitions of attacks. The brief literature review on detection and prevention of security attacks is presented in Section 3.Finally Section 4 concludes the paper.

2. ATTACKS IN MANET

Attacks in MANET can be classified as Active and Passive attacks. An Active attack is one in which an attacker which is an authorized node destroy or alter the data that is being exchanged in the network. While a Passive attack attacker node which is an unauthorized node get the data without disrupting or damaging the network operation.

Another classification can be External and Internal attacks. In External attacks the attacker node is one which do not belong to that network while in Internal attacks the Attacker node belongs to that network. Internal attacks are more severe than External attacks since attacker knows all secret information and have privileged access rights.

Many security issues such as snooping attacks, wormhole attacks, black hole attacks [16], routing table overflow, poisoning attacks, packet replication, and denial of service (DoS) attacks, distributed DoS (DDoS) attacks [17] have been studied in the recent years. The misbehavior routing problem [18] is one of the popularized security threats such as Black hole attacks. Some researchers propose their secure routing ideas [19-21] to resolve this issue, but the security problem is still an issue.

Attacks can also be classified on layered basis. Each layer undergoes different kind of attacks. Table 1 shows common type of attacks on various layers.

Table 1. Type of attacks on layers

Layer	Attacks
Physical layer	Jamming, interceptions, eavesdropping
Data link layer	Traffic analysis, monitoring
Network layer	Wormhole, Black hole, Gray hole, message tempering, Byzantine, Flooding, resource consumption, location disclosure attacks
Transport layer	Session hijacking, SYN Flooding
Multiple layer	Denial of Service (DoS), man-in-the-middle attack

Restricting on network layer in [10] [11] [13] various network layer attack types are considered. Here some of them are discussed.

2.1 Gray Hole Attack

In this kind of attack a malicious node does not participate in route discovery mechanism that is initiated by other nodes and is therefore not a part of active route. Such malicious nodes would increase the route discovery failure and harm the overall network performance [10]. Another intention of such attackers is to conserve their energy by interpreting the message intended for them only and otherwise they do not cooperate with other nodes, which ultimately degrade the performance of the network.

2.2 Black Hole Attack

In this kind of attack a malicious node participate in route discovery mechanism by sending RREP message that includes the highest sequence number and this message is perceived as if it is coming from the destination or from a node which has a fresh enough route to the destination [8]. The source then starts to send out its data packets to the black hole trusting that these packets will reach the destination. As soon as the data transmission starts, malicious node drops the data packets that are needed to be forwarded to destinations. Black hole attack is more destructive as compared to gray hole attack.

2.3 Message Tempering

In this kind of attack an intermediate node behaving as malicious node delete or add some bytes in the data packet received by him to forward to the destination. This change in data may cause abnormalities or destruction in network.

2.4 Byzantine Attack

This attack can be done by a single intermediate node or a group of intermediates nodes, behaving as malicious nodes they either create a routing loop or direct the data packets to non optimal path or selectively drop the packets. Such attacks are difficult to identify.

2.5 Flooding Attack

In this attack malicious node floods the network with the unnecessary data packets. The victim nodes are not able to receive or forward any data packet and thus any data packet forwarded to such nodes is discarded from the network.

2.6 Wormhole Attack

In this wormhole attack a malicious node receives packets at one location in the network and tunnels them to another location in the network, where these packets are resent into the network [2]. Due to broadcast nature of the radio channel the attacker may create a wormhole for those packets also that does not belong to him.

2.7 Information Disclosure

In this attack any authorized node act as a malicious node by leaking the confidential or important information to the other unauthorized nodes. Information can be of type location, route, public /private keys or password related in details.

2.8 Resource Consumption Attack

Here resources are basically battery power, computation power, bandwidth which is limited. In this attack malicious node target these resources in an intention to waste them. This could be done by attacker node through forwarding stale packets to nodes, generating beacon packets frequently or by requesting for routes. If malicious node use the battery power of another node by keeping node busy by pumping packets one by one again and again then such attack is known as sleep deprivation attack.

2.9 Routing Attacks

These kinds of attacks affect the normal operation of the routing protocol used in the network. Routing attacks can be of several types as:

2.9.1 Packet Replication Attack

In this attack the malicious node replicate the stale packet and forward to the other node on order to use the battery power and consume bandwidth and create confusion in the routing process.

2.9.2 Routing Table Overflow

In this attacker node create routes for non relevant node with an intension that no new routes are created. This causes an overflow of routing tables.

2.9.3 Routing Table Poisoning

In this malicious node propagate untrue routing updates or modify route update packet sent to other nodes. This may cause inaccessible of some part of network, sub-optimal routing or congestion in the network’s portions. If the malicious node poison the routing table/cache in which information about routes is maintained then such attack is known as Route Cache Poisoning.

2.9.4 Rushing Attack

In this when attacker node receive any request packet for route discovery then it sends the packet in the whole network before any other node forward the request packet. Due to this if same request packet send by authorized node to already received nodes then they consider packet as duplicate and discard it. In this way attacker will always be part of the route and it is extremely difficult to identify such malicious node.

2.9.5 Selfish Behavior

In this attacker node selfish participate in route discovery mechanism and become a part of an active route. As it becomes the part of an active route, the attacker nodes would start dropping data packets that are not related to him with an intension to conserve energy which is required to forward data packets that belongs to other nodes.

3. RELATED WORK

3.1 Preventing Black and Gray Hole Attacks in AODV using Optimal Path Routing and Hash

Hizbullah Khattak et al. [1] propose to use the second optimal route for data packets transmission and hash function for black and gray holes attacks avoidance and data integrity. Here author discard the very first optimum reply and choose the second shortest route reply message to establish route from source to destination. This solution avoids black hole / gray hole attacks in such a way that by using the second shortest path for data packets transmission, it would be hard for black hole or gray hole node to monitor the entire network to know where to place itself in a network and mislead the source node that it has the second shortest route to the destination [1]. A hash function in case of many malicious nodes in the network is used. While sending data packets to destination, source also sends the hash value of the message. On receiving all the data packets destination compute hash value and if both the values found equal means the is no black hole/ gray hole attack. If in case of attack destination node broadcast data packet error message and source saves this route in the table so as to avoid in future and rebroadcast route request message.

3.2 Intrusion Detection and Defense mechanism for Packet Replication Attack over MANET Using Swarm Intelligence

G. Indirani et al. [2] proposed a defense mechanism based on DSR algorithm having two extensions Watchdog and Pathrater. Watchdog module identify the misbehaving node by keeping a watch on node that it forward the packet to next node, if node does not forward the packet then it is considered as misbehaving node and is reported. Pathrater uses this information given by watchdog module and deletes the corresponding route from the route table and determine another route available to the destination by looking in its cache table. If no route available then Pathrater will broadcast a Route Request to get a new route to the destination.

3.3 Reduction of Delays in Reactive Routing Protocol for Unobservable Mobile Ad-Hoc Networks

In [3] the sequence number identification method to avoid the black hole attacks in MANET is used. Each packet has a unique sequence number and recent packet must have greater sequence number that it's pervious packet. At the arrival or transmission of packet routing table is updated. Source initiate transmission by broadcasting RREQ. After reaching the RREQ to the destination, it can initiate a RREP to the source node, and RREP hold the last packet-sequence-numbers received from this source node [3]. An intermediate node on receiving RREQ can send RREP to source enclosing last packet sequence number received from source node by this intermediate node. Now if this intermediate node act as a black hole node then it will continuously send RREP to source and thus it can be identified since it will not have the previous destination sequence number. In this way attacker can be easily identified and remove from the network.

3.4 GAODV: A Modified AODV against single and collaborative Black Hole attacks in MANETs

Sanjay K. Dhurandher et al. [4] uses a modified AODV protocol known as GAODV protocol. To detect the presence of black hole special control packets, CONFIRM, CHCKCNFRM and REPLYCONFIRM, are used. On receiving RREQ the intermediate nodes that have route towards destination send RREP to source and unicast CONFIRM to destination. For conformation source unicast CHCKCNFRM to destination and in response destination broadcast REPLYCONFIRM only if destination receives CONFIRM and CHCKCNFRM. A black hole node does not have route towards destination and will not be able to send CONFIRM and thus reply to CHCKCNFRM is never generated by destination. Source concludes that RREP sending node is a black hole node and is thus rejected.

3.5 Wormhole Attack Avoidance Technique in MANET

In [5] DSR protocol is modified to detect and prevent wormhole nodes in an ad hoc network and also to select the alternative path by using route discovery method. After detecting a wormhole node it fires the message in the path without affecting performance of network. Modified DSR detects such nodes and the routes which contains the misbehaving nodes, are simply dropped and not added into the routing table of the DSR so that in future that routes are not used in any communication.

3.6 MR-AODV: A Solution to Mitigate Blackhole and Grayhole Attacks in AODV Based MANETs

Rutvij H. Jhaveri [7] proposed a protocol MR-AODV which is modification of R-AODV. MR-AODV establishes the secure route for data transmission by detecting black hole and gray hole nodes during route discovery phase. As soon as malicious node is detected MR-AODV updates the routing table with malicious node entry and discards RREP. MR-AODV does not forward on reverse path and also it does not require any flag. Thus RREP indicating shortest fresher path will be chosen for data transmission by the source node. MR-AODV reduces overhead by not forwarding RREP after detection of misbehavior.

3.7 PPN: Prime Product Number based Malicious Node Detection Scheme for MANETs

The method of detection and removal of malicious node by using prime product number (PPN) is used in [6]. In this scheme each node has unique prime number. Source node (SN) broadcast RREQ to destination and in response intermediate node (IN) wishing to send RREP has to provide product of all prime numbers (PPN) from destination to source and also information of its cluster head. Upon receiving the RREP message from IN, SN with the help of its cluster head (CH) will divide the PPN with the Node IDs stored in neighbor table at CH to see whether IN is its reliable node [6]. If PPN is fully divisible, then intermediate node is a reliable node, else it is malicious node and CH adds it to malicious list and broadcast it to whole network to remove it from the routing table.

3.8 An Efficient Prevention of Black Hole Problem in AODV Routing Protocol in MANET

The proposal in [9] uses promiscuous mode of the node. This mode allows a node to intercept and read each network packet that arrives in its entirety [9]. Source node broadcast RREQ message in network. On receiving RREP message from destination a route is established and if RREP message is received from intermediate node then a node proceeding to the node which send RREP message switches to promiscuous mode and sends hello message to the destination node through this node. If the hello message is forwarded by this node to the destination, the node and hence the route is safe; otherwise, the node is a malicious node [9].The preceding node informs about the malicious node in the network.

3.9 Black Hole Attack in Mobile Ad Hoc Networks

Al-Shurman et al. [13] proposed two solution two solutions to detect the black hole attack. In the first solution, a path will be selected among all received routes, in terms of shared hops. From the shared hops the source node can recognize the safe route to the destination. The main drawback of this approach is to force more delay on the network. In the second solution, each node stores the last-packet-sequence-numbers for the last packet sent to each node and the last-packet-sequence-numbers for the last packet received from each node. The received RREP contains last-packet-sequence-numbers received from the source node. According to the sequence number, the source node can detect the malicious RREP.

4. CONCLUSION AND FUTURE WORK

Due to the inherent design disadvantages of routing protocol in MANETs, many researchers have performed diverse techniques to propose different types of prevention mechanisms for malicious attacks. In this paper, we first summarized the MANET and classified popular routing protocols in such networks. Then, few attacks along with a latest survey of existing solutions are categorized and discussed. The various authors have given various proposals for detection and prevention of malicious attack in MANET but every proposal has some limitations in their respected solutions. These procedures are unable to analyze and detect possible collaborative attacking nodes. The malicious attack is still an active research area. This paper will benefit more researchers to realize the current status rapidly. Future work includes intend to develop simulations to analyze the effects of few such attack type and analyze the performance of the proposed solutions and compare their performances.

5. ACKNOWLEDGMENTS

I sincerely thank to my honorable guide Prof. Anand Motwani and others who have contributed towards the preparation of the paper.

6. REFERENCES

[1] Hizbullah Khattak, Nizamuddin, Fahad Khurshid, Noor ul Amin, ” Preventing Black and Gray Hole Attacks in AODV using Optimal Path Routing and Hash”,(645-648) 978-1-4673-5200-0/13/2013 IEEE.

[2] G. Indirani, Dr. K. Selvakumar, V. Sivagamasundari, “Intrusion Detection and Defense Mechanism for Packet Replication Attack over MANET Using Swarm Intelligence”, (152-156) Pattern Recognition, Informatics and Mobile Engineering (PRIME) February 21-22, 978-1-4673-5845-3/13/2013 IEEE.

[3] P.Karthikkannan, K.P.Lavanya Priya,” Reduction of Delays in Reactive Routing Protocol for Unobservable Mobile Ad-Hoc Networks”, 2013 IEEE.

[4] Sanjay K. Dhurandher, Isaac Woungang, Raveena Mathur , Prashant Khurana,” GAODV: A Modified AODV against single and collaborative Black Hole attacks in MANETs”,(357-362) 2013 27th International Conference on Advanced Information Networking and Applications Workshops, 978-0-7695-4952-1/13/2013 IEEE.

[5] Yudhvir Singh, Avni Khatkar, Prabha Rani, Deepika, Dheer Dhwaj Barak ,“Wormhole Attack Avoidance Technique in Mobile Adhoc Networks”,(283-287) 2013 Third International Conference on Advanced Computing & Communication Technologies, 978-0-7695-4941-5/13/ 2013 IEEE

[6] Sapna Gambhir and Saurabh Sharma,” PPN: Prime Product Number based Malicious Node Detection Scheme for MANETs”, (335-340) 2012 3rd IEEE International Advance Computing Conference (IACC), 978-1-4673-4529-3/12/ 2012 IEEE.

[7] Rutvij H. Jhaveri, “MR-AODV: A Solution to Mitigate Blackhole and Grayhole Attacks in AODV Based MANETs “, (254-260)2012 Third International Conference on Advanced Computing & Communication Technologies, 978-0-7695-4941-5/12 / 2012 IEEE.

[8] Roopal Lakhwani , Vikram Jain , Anand Motwani , “ Detection and Prevention of Black Hole Attack in Mobile Ad-Hoc Networks”, International Journal of Computer Applications (0975 – 8887) Volume 59– No.8, December 2012.

[9] Pramod Kumar Singh, Govind Sharma,” An Efficient Prevention of Black Hole Problem in AODV Routing Protocol in MANET”,(902-906) 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, 978-0-7695-4745-9/12/ 2012 IEEE.

[10] Mohammed Saeed Alkatheiri, Jianwei Liu, Abdur Rashid Sangi, ” AODV Routing Protocol Under Several Routing Attacks in MANETs” ,2011 IEEE, 978-1-61284-307-0/11.

[11] Htoo Maung Nyo, Piboonlit Viriyaphol, ” Detecting and Eliminating Black Hole in AODV Routing”, 2011 IEEE, 978-1-4244-6252-0/11

[12] S.Kurosawa, H.Nakayama, N.Kat, A.Jamalipour, and Y.Nemoto, "Detecting Blackhole Attack on AODV based Mobile Ad Hoc Networks by Dynamic Learning Method", International Journal of Network Security,Vo1.5, No.3, P.P 338-346, Nov. 2007

[13] Al-Shurman, M. Yoo, S. Park, “Black hole attack in Mobile Ad Hoc Networks”, in Proc. ACM Southeast Regional Conference, pp. 96-97, 2004.

[14] Zhou L, Chao H-C, “Multimedia Traffic Security Architecture for the Internet of Things” IEEE Network 25(3):29–34. IEEE 2011.

[15] 8. Yang H, Lou H, Ye F, Lu S, Zhang L (2004) Security in Mobile Ad Hoc Networks: Challenges and Solutions. IEEE Wireless Communications 11(1):38–47.

[16] Umang S, Reddy BVR, Hoda MN, “Enhanced Intrusion Detection System for Malicious Node Detection in Ad Hoc Routing Protocols using Minimal Energy Consumption”, IET Communications 4(17):2084–2094. 2010.

[17] Wu B, Chen J, Wu J, Cardei M, “A Survey of Attacks and Countermeasures in Mobile Ad Hoc Networks” In: Xiao Y,Shen X, Du D-Z (eds) Wireless Network Security. on Signals and Communication Technology. Springer, New York 2007.

[18] Marti S, Giuli TJ, Lai K, Baker M, “Mitigating Routing Misbehavior in Mobile Ad Hoc Networks” 6th annual International Conference on Mobile Computing and Networking, Boston, Massachusetts, August 2000.

[19] Tseng Y-C, Jiang J-R, Lee J-H, “Secure Bootstrapping and Routing in an IPv6-based Ad Hoc Network”, Journal of Internet Technology 5(2):123–130, 2004.

[20] Hu Y-C, Perrig A, Survey of Secure Wireless Ad Hoc Routing. IEEE Security & Privacy 2(3):28–39, IEEE 2004.

[21] Raja Mahmood RA, Khan AI, “A Survey on Detecting Black Hole Attack in AODV-based Mobile Ad Hoc Networks, International Symposium on High Capacity Optical Networks and Enabling Technologies, Dubai, United Arab Emirates, November 2007.