ijecs open access www.ijecs.in

International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 3 Issue 6 June, 2014 Page No. 6735-6738

Black Hole Attack Prevention Techniques in MANET: A Review

Deepak Mishra, Mr. Srinivas Arukonda

Research Scholar (M.Tech.)

Computer Science and Engineering Greater Noida,UP, India

Asst. Professor (Dept. Of Computer Science) Galgotias University, Greater Noida,UP, India

Abstract:

Mobile ad-hoc networks (MANET) is a major next generation wireless technology. Dynamically and arbitrarily located nodes communicate to each other to form a Mobile Adhoc Network. MANET is more vulnerable to various types of attack than wired network. Black hole attack is more severe threat to MANET than any other attack. Prevention of Black hole attack is done by finding the malicious node before any harm can be done. Different techniques are proposed to prevent this type of attack. In this paper these techniques are studied with their advantages and disadvantages.

Keywords: mobile ad-hoc network, securing ad-hoc network, intrusion prevention, black hole attack

1. Introduction:

Mobile Adhoc NETworks (MANET) are the networks of mobile computing devices connected wirelessly without any support of fixed infrastructure. There are some characteristics of MANET, which are as follows:

- No need of fixed infrastructure
- Topology of the network is dynamic
- Two node communicate directly if they are within radio range
- Less Secure than wired network
- MANET is an autonomous system of mobile node. It can operate in isolation or may have gateways to and interfaces with a fixed network.
- There are Bandwidth Constraints and Energy Constraints
- Distributed nature of operation for security, routing and host configuration.
- More scalable than Fixed Network.
- High user density and large level of user mobility
- Nodal connectivity is intermittent.
- Each node act as both host and router

2. Type of MANET:

- *Intelligent Vehicular Adhoc Network (InVANET):* It uses artificial intelligence to tackle unexpected situation like vehicular collision and accidents. InVANET focuses on the application to improve vehicular safety by taking into account the physiological and ecological based context-aware sensitive parameters as intelligence hence increasing driver convenience.
- *Vehicular Adhoc Network(VANET):*Enable effective communication with another vehicle or help to communicate with roadside equipment.A VANET turns every participating car into a wireless router or node, allowing cars approximately 100 to 300 meters of each other to connect and, in turn, create a network with a wide range. As cars fall out of the signal range and drop out of the network, other cars can join in, connecting vehicles to one another so that a mobile Internet is created.
- *Internet based Mobile Adhoc Network (iMANET):* Helps to link fixed as well as mobile nodes. In such type of MANET normal adhoc routing algorithms don't apply directly

3. Issues in MANET:

3.1 Randomly Changing Topology: Topology of MANET keeps changing over the time. So one protocol that is suited for one topology can't work next time when topology gets changed. The Nodes work in a nomadic environment where they are allowed to join and leave the wireless network. When a node comes in the radio range of a node it will be able to communicate with that node.

3.2 Limited Energy: The node present in the mobile adhoc network has limited battery power for their operation. It is assumed that there is no alternate power source. The malicious node can sent huge traffic to the target node to make it busy in handling the packets. Due to this the node consumes more power and at last gets exhausted. Thus the target node will not be able to provide services.

3.3 No centralized control: There is no centralized control in MANET. This leads to many security problems. Each node behaves as server as well as client. Traffic monitoring becomes extremely difficult in distributed and randomly changing environment of MANET. The attacker can easy take advantage of this drawback. Some algorithms in MANET rely on cooperative participation of all nodes and infrastructure. Since there is no centralized authority and the decision making is decentralized, the attacker can make use of this vulnerability and perform some attacks that can break the cooperative algorithms.

3.4 Scalability: Any node that comes into the radio range of network can easily join or leave the network at any time. Therefore it is very difficult for anyone to predict the exact number of node present in network at any time. The protocols that are applied to the ad-hoc network should be compatible to the continuously changing scale of the ad hoc network.

3.5 Threat from Compromised node inside network: Mobile mode can join and leave the network freely; it is hard for node to work out some policies to prevent the possible malicious behavior. Due to mobility nature of MANET a malicious node can frequently change its target thus it is very difficult to identify malicious node in large network. Therefore, Threats from malicious node inside the network is much more severe than the threats from outside the network.

4. Security Criteria:

There are some security criteria of MANET which ensure the safety of network. Some are as follows [8]:

4.1 Availability: It refers to the property of the network to continue provide services.

4.2 Integrity: There should be no modification in message when it reaches to destination node.

4.3 Confidentiality: The message can't be viewed in its original form by any unauthorized user.

4.4 Authenticity: This ensures that the destination nodes are genuine not impersonate.

4.5 Authorization: Using this property different access rights are assigned to different types of users.

4.6 Non Repudiation: This property ensures that the sender and receiver cannot disavow about sending and receiving the message.

4.7Anonymity: The information related to the identity of a node should be kept to preserve privacy.

5. Routing Protocol:

There are many routing protocols in MANET. Whenever a node wants to communicate with target node, it broadcast its current status to neighbors. Routing protocols can be classified into proactive, Reactive and Hybrid routing protocol.

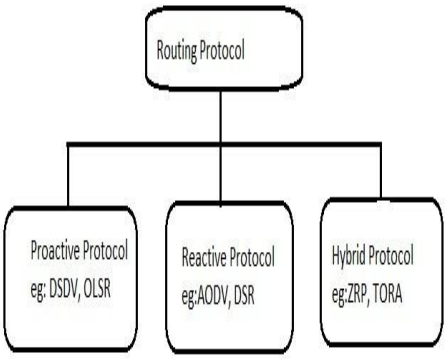

Fig: Classification of Routing Protocols

5.1 Proactive Routing Protocol: This is a table-driven routing protocol. Each node maintains a routing table which not only contains record of adjacent nodes and reachable nodes but also the number of hops. If the size of network increases, the overhead also increase which results in decline in performance. Destination sequenced distance vector (DSDV) and Optimized link state routing (OLSR) are proactive protocol.

*5.2 Reactive Routing Protocol:*This protocol is also called on-demand routing protocol. When a node want to transmit data packet the reactive protocol started. The advantage of this protocol is that wasted bandwidth induced from cyclically broadcast gets reduced. The main disadvantage of this protocol is that it leads to packet loss. Adhoc on-demand distance vector (AODV) and Dynamic Source Routing (DSR) are the example of reactive routing protocol. In AODV, each node records the information of next hop in its routing table. The route discovery process executed when the destination node can't be reached from source node. The source node broadcasts the route request (RREQ) packet to start route discovery process. All the node receive the RREQ packets sends the route reply (RREP) packet to the source node if the destination node information is occurred in their routing table. Route Maintenance process is started when the network topology has changed or the connection has failed. The source node is informed by a route error (RRER) packet. In DSR nodes maintains their route cache from source to destination node. Performance of DSR decreases with the mobility of network increases, a lower packet delivery ration within the higher network mobility.

5.3 Hybrid Routing Protocol: This protocol contains the advantages of proactive and reactive protocol. Proactive protocol is used to gather the unfamiliar routing information, then reactive protocol is used to maintain the routing information when topology changes. Zone Routing Protocol (ZRP) and Temporally-ordered Routing Algorithm (TORA) are the example of hybrid protocol

6. Attacks in Mobile Adhoc Network:

There are two types of attack in MANET.

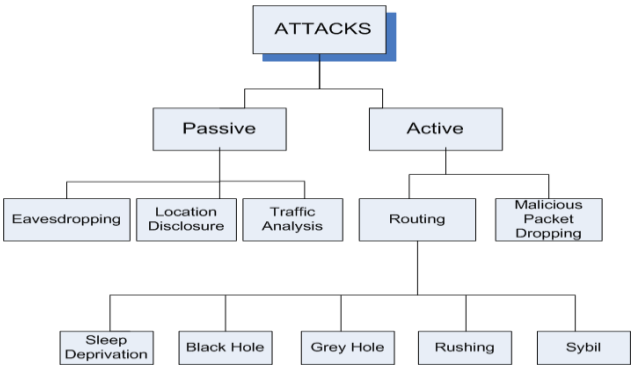

Fig. Classification of network layer attacks in MANETs[9]

- *Passive Attacks:* In the passive attack the attacker does not disturb the operation of routing protocol instead it try to capture vital information via traffic analysis. Due to this type of attack the confidentiality of message is compromised. Passive attacks include Eavesdropping, Location Disclosure, and Traffic analysis.
- *Active Attacks:* In active attacks the intruders modify, inject, forge, fabricate or drop data packet. This results in loss of integrity of data packet. Active attack disturb the operation of the network and more severe than the passive attack. Active attack can be further divided in packet dropping attack and routing attack. In MAET when any node wants to send a data packet to another node it send the packet to next node and next node forward this data packet to its next node in the path. It is very important that the intermediate node forward the data packet to next node. Packet dropping attack happens when any malicious node instead of forwarding the data packet drop the packet. Routing attacks include Sleep Deprivation, Black Hole, Grey Hole, Rushing and Sybil attack. In the network when any node does not interact with other node it switch into sleep mode to preserve its energy. In the sleep deprivation, an attacker interacts with the node in a manner that appears to be legitimate, but the purpose of the interaction is to keep the victim node out of its power-conserving sleep mode. In the Black hole attack the malicious node claims to have shorted route to destination when a packet arrive it discard the packet instead of forwarding it. In the Grey hole attack the malicious node drop some of the packet and forward or misroute other packet. Each node in a MANET requires a unique address through which nodes are identified. In the Sybil attack, the attacker could use either random identities or the identity of another node to create confusion in routing process or to establish bases for some other attack. The motive behind launching either packet dropping or routing attacks is to achieve a certain goal such as denial of service. Other goals of intruders include partitioning the network, creating routing loops, discovering valuable information, or left of resources.

Black Hole Attack:

Black hole attack is a kind of active attack in which the malicious node takes the benefits of the vulnerabilities of routing protocol. In Black hole attack the malicious node advertise itself as having the shortest path to the destination. When packet arrived at the malicious node it discards it instead of forwarding it to next node.

There are two types of black hole attack:

Single Black hole attack: It is very simple form of black hole attack. In this only one malicious node is used to carry out the attack. That malicious node advertises itself as a node of shortest path and when packed arrived at it, node simply discards the packet.

Cooperative Black hole attack: In this attack two or more malicious nodes work together to carry out the attack. This is much more complex and damaging than the single black hole attack.

Many techniques are proposed to avoid and detect the black hole attack in MANET. In the following, some of these techniques are presented with their advantage and disadvantages.

In [1] authors proposed two solutions for black hole attack avoidance. In first solution they find more than one route to destination and the second solution involve the exploitation of the packet sequence number included in any packet. The problem with the first solution is the time delay and non-existence of sharp nodes or hops between nodes. The second solution is fast and reliable way to identify the suspicious node. In it every node should have maintain two table, one to keep last packet sequence number for every last sent to every node and another to keep last packet sequence number for the last packet received from every node. In this paper authors only studied one node attack. The group of attack for this problem should be studied.

In [2] authors studied different techniques to detect black hole attack with their advantages and disadvantages. Authors discuss two types of black hole attack, one is Single node black hole attack and another is Cooperative black hole attack. In this paper the authors also discuss briefly about the techniques like watchdog & path rater , Jaydip Sen and Harish Reddy's solution for Gray hole attack and TRIPO techniques. They concluded that TRIPO is better techniques. It not only

detect and punishes the attacker node but also stimulate network nodes to relay other nodes packet.

BAAP (Black hole Avoidance Protocol for wireless network) [3] avoid black hole attack without any use of special hardware and dependency on physical medium of wireless network. This protocol uses AOMDV (Adhoc On demand multipath distance vector). In this protocol every node maintains the legitimacy of their neighbor nodes to form the correct path to destination node. In path discovery, an intermediate node will attempt to create a route that does not go through a node whose legitimacy ratio crosses the lower threshold level. To evaluate the performance of this algorithm some performance matrices are used which are Packet Delivery Ratio, Route Formation Delay, Node Speed, Pause Time. Packet loss in AODV are more than 90% while in BAAP it is only 15.6%-21.3% in presence of 2-3 malicious nodes. In the absence of malicious node this protocol require little more time. Packet Loss increases as mobility increases.

In [4] authors compare the performance of two security techniques of MANET i.e. intrusion detection system and watchdog & path rater, under partition method attack. The performance matrices used to evaluate are availability factor and Integrity factor. The result shows that the Availability measure of IDS is better than WPR and Integrity measure of WPR is better than IDS. In this paper author uses only Uni-cast MANET and does not consider other type of passive and active attack.

In [5] authors give emphasis on how SMC solutions can be used for privacy preservation during computation. SMC is short form of Secure Multiparty computation. Sometimes the physically distributed computing devices in a network may be interested in computing some function of their private inputs without disclosing these inputs to one another. This type of computation falls under the category of Secure Multiparty Computation (SMC). The solution to SMC problems in Mobile Ad hoc Networks (MANET) can be found with the modification of the data inputs or with some anonymization technique. In this paper authors also discussed various security issues, security criteria of MANET.

In [6] authors proposed a new intrusion detection system named Enhanced Adaptive ACKnowledge (EAACK) specially designed for MANETs. In this paper authors also gives the advantages and disadvantages of three existing techniques, namely, Watchdog, TWOACK, Adaptive ACKowledment. EAACK tackle three weakness of watchdog scheme, namely, false misbehavior, limited transmission power, and receiver collision. In this paper authors implemented both DSA and RSA in proposed EAACK and compare their performance in MANET. The performance matrices used to evaluate the performance of proposed scheme are Packet Delivery Ratio (PDR) and Routing Overhead (RO).In the conclusion they show that the
EAACK is the only scheme that is capable of detecting false misbehavior report. DSA scheme always produces less slightly less overhead than RSA does. DSA is more desirable digital signature scheme in MANETs. EAACK prevent attackers from initiating forged acknowledgment attack.

In [7] authors proposed a FUZZY LOGIC based mechanism to detect the black hole attack in MANET with AODV protocol. The performance matrices used to evaluate the performance are Loss rate, Transmission Rate and Network Delay. The Fuzzy Logic based mechanism improve the performance and throughput of the system. This Fuzzy Logic based mechanism can also be used againsed Gray hole, Worm hole, Denial Of services attack etc.

Conclusion:

The overview of MANET is presented in this paper. After that various types of security issues and attacks in MANET are discussed. Various routing protocols are also presented briefly. Works of various authors in the field of black hole attack is discussed with the merits and demerits. It is observed that, in the various techniques presented, no one is reliable. Many researches are ongoing to find the more effective and more reliable solution to the black hole attack. Therefore the future work include the finding the best techniques to prevent and detect black hole attack.

References:

[1] Mohammad Al-Shurman, Seong-Moo Yoo,"*Black Hole attack in Mobile ad-hoc Networks*".

[2] Hardik Bhanabhai Patel, Prof Jwalant Baria, "*Black Hole attack in Mobile Adhoc network*"

[3] Saurabh Gupta, Subrat Kar, S.Dharmaraj, "*BAAT:Black hole Attack Avoidence Protocol For Wireless Network*",International Conference on Computer and Communication Technology (ICCCT)-2011.

[4]Maitha Salem Al Mazrouei, Dr Sundaravalli Narayanaswami,"*Mobile Adhoc Networks: A Simulation based Security Evaluation and Intrusion Prevention*",6th International Conference on Internet Technology and Secured Transactions, 11-14 December 2011

[5] Rashid Sheikhl, Mahakal Singh Chandee, Durgesh Kumar Mishra, "*Security Issues in MANET: A Review*",2010

[6] Elhadi M. Shakshuki, Nan Kang, and Tarek R. Sheltami, "*EAACK—A Secure Intrusion-Detection System for MANETs*", IEEE TRANSACTIONS ON INDUSTRIAL ELECTRONICS, VOL. 60, NO. 3, MARCH 2013

[7] Swati Saini, Vinod Saroha,"Analysis and Dtection of Black hole attack in MANET",IJSR Volume 2 Issue 5, May 2013

[8] Rashid Sheikh, Mahakal Singh Chandel, Durgesh Kumar Mishra,"*Security Issues in MANET: A Review*",IEEE 2010.

[9] Adnan Nadeem, Michael P. Howarth, " *A Survey of MANET Intrusion Detection &*
Prevention Approaches for Network Layer Attacks", IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 15, NO. 4, FOURTH QUARTER 2013