THE ROUTING PROTOCOLS AND SECURITY ISSUES IN MANET

Asha Rani & Dr. Gaurav Aggarwal

[1]Research Scholar, [2]Associate Professor & Head,
Jagannath University, NCR, Haryana.

Abstract: MANET is an association of large no. of sensor nodes and having self-directed commands using the unprotected wireless connection. The individual needs in the network can accompany and leave the network without any permission. MANET is an infrastructure less network. The network topology is rapidly changed due to nodes mobility, resource constraints and bandwidth limitation of wireless medias. This nature of nodes leads to different type of security threats. MANET suffers from disruption so that nodes are not able to take part in path finding method with a target to spoil full network functioning. A no. of protocols has been found for efficient routing. There are many types of securities attack which disturb the network operation. In this paper, we focus on many proposed routing protocol for MANET, types of security attacks and a survey on existing techniques of detection and prevention of attacks is presented

Keywords: MANET, Security, Black Hole Attack & Grey Hole Attack.

Introduction

MANET is a wireless network formed by collection of mobile nodes without the preset infrastructure. When network topology changes nodes in range is still connected. The major shortcoming is their limited bandwidth, memory, processing capabilities and open medium and so these are more prone to malicious attacks [8]. MANET 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.

MANET has a wide usage. That's why there are several open issues about it, 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 network [4].

Routing protocol is principally a standard that decide the behavior of the node in the context to route the data packet from one node to another. Routing protocol can be classified as link state protocol and distance vector protocol. Link state protocol build the topology of the entire network for calculating routes and then calculate the best path. These protocols consume more power and memory resources. DLSR and OLSR are examples of such protocols. While in distance vector protocol router keeps information of their neighbors only and calculates the cost based on it. AODV is the example of this type of 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 example 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 the example of it. Hybrid routing protocol as the 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 (ZSR) is one of the hybrid protocols.

In rest of the paper, Section 2 is introducing the classification and definition of attacks. Section 3 briefly discussed about the literature review on detection and prevention of security attacks. Finally, section 4 concludes the paper.

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 attack,** the attacker node is one which does not belong to the network while in **Internal Attacks** the attacker node belongs to the 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 [8], routing table overflow, poisoning attacks, packet replication and denial of services attack (DoS) have been studied in recent years.

Attacks can be classified on layered basis. Each layer undergoes different kind of attacks. Table 1 shows different kinds of attack.

Table 1. Types of attacks on layers

Layers	Attacks
Physical layer	Jamming, Interception, eavesdropping
Data link layer	Traffic Analysis, monitoring
Network layer	Wormhole, black hole, Gray hole, message tempering, flooding, Resource consumption, location disclosure attack
Transport layer	Session Hijacking, SYN flooding
Multiple layer	Denial of services(DoS), Man in the middle attack

2.1 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 coming from the destination or from a node which has a fresh enough route to the destination [6]. The source then starts to send out its data packets to the black hole trusting that this packet will reach the destination. As soon as the data transmission starts, malicious nodes drop the packets that are needed to be forwarded to the destination. Black hole is more destructive as compared to gray hole attack.

2.2 Gray hole attack

In this 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 nodes would increase the route discovery failure and harm the overall network performance [5]. Another intention of such attacker 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 network.

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 Worm hole attack

In this attack a malicious node receives packet 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 radio channel the attacker may create a wormhole for those packets also that does not belong to him.

LITERATURE REVIEW ON DETECTION AND PREVENTION OF SECURITY ATTACKS

Wormhole Attack Avoidance Techniques 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 the wormhole node, it fires the message in the path without affecting the 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.

Preventing Black and Grey hole attacks in AODV using optimal path routing and Hash

Here we 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 second shortest path for data packets transmission, it would be hard for black hole or gray hole nodes 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 path to the destination [1]. A hash function in case of many malicious nodes in the network is used. While sending data packets to the destination, source also sends the hash value to the message. On receiving all the data packets destination computes hash value and if both the values found equal means there 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.

Intrusion Detection and defense mechanism for Packet Publication attack over MANET Using Swarm Intelligence

G. Indirani [2] proposed a defense mechanism based on DSR algorithm having two extensions Watchdog and Path rater. Watchdog module identify the misbehaving node by keeping a watch on node that it forward the packet to the next node, if node does not forward the packet then it is considered as misbehaving node and is reported. Path rater 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 Path rater will broadcast a route request to get a new route to the destination

An efficient prevention of black hole problem in AODV routing protocol in MANET

The proposal in [4] uses promiscuous mode of the node. This mode allows a node to intercept and read each network packet that arrives in its entirety. 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, the node and hence the route is safe; otherwise the node is a malicious node. The proceeding node informs about the malicious node in the network.

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 is used in [3]. 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 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 the neighbor table at CH to see whether IN is its reliable node [3]. If PPN is fully divisible, then intermediate node is 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.

CONCLUSIONS

Due to inherent design disadvantages of routing protocol in MANETs, many researchers have performed diverse techniques to purpose different types of prevention mechanism for malicious attacks. In this paper, we first summarized the MANET and classified popular routing protocol in such network. Then few attacks along with a latest survey of existing solution are categorized and discussed. The various authors have given various proposals for detection and prevention of malicious attacks but every proposal has some limitations in their respected solution. 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 simulation to analyze the effects of few such attack type and analyze the performance of proposed solutions and compare their performance.

REFERENCES

[1] Hizbullah khattak, Nizamuddin, Fahad Khursid, “Preventing Black and Gray hole attack in AODV using optimal path and routing hash”

[2] G. Indiriani, Dr. K. Selvakumar, "Intrusion detection and defense mechanism for packet replication attack over MANET using Swarm Intelligence," pattern recognition, informatics and mobile engineering.

[3] Sapna Gambhir and Saurabh Sharma, "PPN: Prime Product Number Based Malicious node Detection scheme for MANETs" International advance computing conference (IACC).

[4] Pramod Kumar Singh, Govind Sharma, "An Efficient prevention of black hole problem in AODV Routing protocol", 11th international conference on trust, security and privacy in computing and communication.

[5] Mohammed Saeed Alkatheiri, Jianwei Liu, Abdul Rashid Sangi, "AODV routing protocol under several routing attacks in MANETs" 2011 IEEE.

[6] Roopal Lakhwani, Vikram Jain, "Detection and Prevention of black hole attack in Mobile ad hoc network" International Journal of Computer Application.

[7] Umang S, Reddy BVR, Hoda MN, "Enhanced intrusion Detection System for malicious node detection in ad hoc routing protocol using minimal energy consumption" IET Communication.

[8] Rutvij H. Jhaveri, " MR-AODV: A solution to mitigate black hole and gray hole attacks in AODV based MANETs" Third International Conference on Advanced Computing and communication technologies.