Study of Layering-Based Attacks in a Mobile Ad Hoc Network

A. VANI

Assistant Professor, ECE Department, CBIT
Hyderabad, Telagana -India

Abstract - Mobile ad hoc networks (MANETs) are more commonly used in military, disaster conditions, rescue operation, etc. Therefore, these networks require a high level of security. It is a most challenging task to provide security for MANETs because of their characteristics. In this situation, lots of work has been realized and most existing security schemes require exhaustive computation and memory, which are the insufficient factors in MANETs. It is very hard to accumulate all requirements in a single security mechanism, as MANETs have severe resources constraints. In this paper, a survey is made on different attacks to which MANETs are exposed as well as the works already realized in this context.

Key Words: MANET, Routing, Attacks, Security.

1. INTRODUCTION

Mobile ad hoc networks (MANETs) consist of hundreds or even thousands of small devices each with processing, and communication capabilities to monitor the real-world environment. Popular Mobile ad hoc networks applications include military, battlefield, rescue operations, so on. Hence, security is a vital issue. One obvious example is battlefield applications where there is a pressing need for secrecy of location and resistance to subversion and destruction of the network. Important security dependent applications include Disasters: In many disaster scenarios, especially those induced by terrorist activities, it may be necessary to protect the location of sufferers from unauthorized disclosure[4]. In Such applications, the availability of the network is never threatened. Attacks causing false alarms may lead to panic responses or even worse, total disregard for the signals.

So, security is a common concern for any network system, but security in MANETs is of immense requirement, hence they should be equipped with security mechanisms to defend against attacks such as node capture, physical tampering, eavesdropping, denial of service, and so on [8]. Providing security for MANETs represents a rich field of research problems, as traditional security mechanisms with high overhead are not applicable for MANETs. This is because these networks are limited in resources and their deployment nature is different from usual networks.
Constraints in MANETs

Some of the major constraints of a MANETs are:

Resource constraints: In MANETs, nodes have limited resources, including low computational capability, small memory, low wireless communication bandwidth, and a limited battery [2].

Transmission range: The communication range of nodes is limited both technically and by the need to conserve energy [1, 3, 2].

Addressing schemes: Due to relatively large number of nodes, it is not possible to build a global addressing scheme for deployment of a large number of nodes as the overhead of identity maintenance is high [1, 3, 2].

Security Requirements
Before discussing, the various possible attacks against MANETs the basic security requirements or goals to achieve are greatly needed. The goal of security services in and their countermeasures is to protect the information and resources from attacks and misbehavior. The security requirements in and their countermeasures, are [2, 8]:
Availability: Ensures that the desired network services are available even in the presence of denial of service attacks.

Authentication: This provides the legitimate communication from one node to another node. In addition, prevents a malicious node that cannot pretend to be as trusted node in the network.

Confidentiality: This ensures that only the desired recipients can understand a given message.

Integrity: Another requirement is messages are not modified in transit by the malicious intermediate nodes.

Non-repudiation: Denotes that a node cannot refuse sending a message it has previously sent.

2. Classification of Attacks

Outsider versus insider attacks:

The outsider attacks regard attacks from nodes that do not belong to a Network. The insider attacks occur when legitimate nodes of a network behave in unintended or unauthorized ways. The inside attacker may have partial key objects and the trust of other nodes. Inside attacks are much harder to detect.

Passive versus active attacks: Passive attacks are in the nature of eavesdropping on, or monitoring of packets exchanged within a network; the active attacks involve several modifications of the data flow or the creation of a false stream in a network[1,3]

3. Physical Layer

This layer is responsible for frequency selection, carrier frequency generation, signal detection, modulation, and data encryption [4].As with any radio-based medium, there exists the possibility of jamming and interferences and causes denial of Service (DoS) attack.

Jamming Attack: This attack generally disturbs the network at physical layer. And in addition this attack adverse the network by knowing the transmission signals used in the network. The intensity of jamming source depends on either to disturb the entire network or portion of the network. The attacker randomly transmits radio signal for communication with the same frequency as the legitimate nodes. The radio signal interferes with other signal sent by a legitimate node and the receivers within the range of the attacker cannot receive any message. Thus, affected nodes become completely isolated as long as jamming signal continues and no messages are exchanged between affected nodes and other nodes [1,4].The adversary adds the unnecessary malicious pockets into the network topology and network traffic is jammed and so the energy of the nodes is decreased. The nodes in the network use certain procedures to change to sleep mode during jamming. The nodes should follow some procedures to switch to sleep mode during jamming.

Denial of Service (DoS) Attack: This type attack caused by the unintentional failure of nodes or malicious action. It is the typical attack against availability. In this attack, the nodes are kept busy by retransmission of legitimate request from other users or inserting new messages in the network. Hence, the nodes occupied and availability of network reduced leading to very slow performance. Attempts of an adversary to disrupt, weaken, or destroy the network as Denial of Service (DoS) attack.

DoS attacks can mainly be categorized into three types:

(1) Consumption of insufficient, limited, or non-renewable resources
(2) Destruction or change of network configuration information
(3) Destruction or change of network resources[3,4]
In addition to this, DoS attacks categorized at each layer and an attacker choose different targets at different layers to stop correct operation of legitimate

4. Network Layer

The important function of network layer is routing messages from one to another node that are neighbors or may be a number of multi-hops away. The routing mechanisms are exploited by several attacks in MANETs[9]. Some common attacks are listed here.

Link Spoofing Attack

This is the most common attack at network layer that directly attack on a routing protocol and mainly focuses on the routing information. This attack makes spoofing, altering and replaying the routing information and consequently the network topology gets confused that leads to the packet loss. In this attack, adversaries may be doing well to create routing loops, repel or attract network traffic, extend or shorten source routes, generate false error messages, divide the network, and increase end-to-end latency etc.

Selective forwarding: In this attack, a compromised or malicious nodes just drops packets of its interest and selectively forwards packets [9].In this attack, the intruder may be interested in suppressing or modifying packets originating from a few selected nodes. In this situation, the adversary reliably forwards the remaining traffic to limit the suspicion of wrongdoing.

A particular variety of this attack is the black hole attack in which a node drops all packets (messages) it receives. Selective forwarding attacks are much harder to detect than black hole attacks. A second protection method is to detect the malicious node or assume that it has failed and search for an alternative route.

Sinkhole Attack

In this attack, an attacker makes a compromised node and it makes more attractive to surrounding nodes by forging routing information [9].This results that surrounding nodes will select the compromised node as the next node to route their data. This type of attack makes selective forwarding and allows all traffic from a large area in the network through the adversary's node

Sybil attack: In this attack, malicious node shows more than one identity to the network [7]. Moreover, it attack has a considerable effect in geographic routing protocols. With this attack the protocols functionality is disrupted by more than one place simultaneously.

Black hole attack

In black hole attack, a malicious node sends route request using routing protocol in order to advertise itself for having the shortest path to the destination node or to the packet it wants to intercept. This attacking hostile node advertises its availability of fresh routes irrespective of checking its routing table. In this way attacker node will always have the accessibility in replying to the route request and thus intercept the data packet and retain it [5, 12].

Wormhole attack: Wormhole is a critical attack, where the attacker receives packets at one point in the network, tunnels them through a less latency link to another point in the network [6, 10]. This convinces the neighbor nodes that these two distant points at either end of the tunnel are very close to each other. If one end point of the tunnel is near to the base station, the wormhole tunnel can attract a significant amount of data traffic to disrupt routing and operational functionality of MANETs. In this case, the attack is similar to a sinkhole attack as the adversary at the other side of the tunnel advertises a better route to the base station.

Hello Flood attack: Many protocols that use hello packets make the naı¨ve assumption that receiving such a packet means the sender is within radio range and is therefore a neighbor. An attacker may use a high powered transmitter to trick a large area of nodes into believing they are neighbors of that transmitting node [11]. Consequently, instead of sending information to the base station, the victim nodes will send them to the adversary's node.

6. Transport Layer

In this layer, end-to-end connections are managed. Two possible attacks in this layer, flooding and DE synchronization, are discussed here:

a. **Flooding**: At this layer, adversaries exploit the protocols that maintain state at either end of the connection. An attacker sends many connection establishment requests to the victim node to exhaust its resources causing the flooding attack.

One solution against this attack is to limit the number of connections that a node can make. But, this can prevent legitimate node to connect to the victim node. Another solution is based on the client puzzles [11]. According to this idea, if a node wants to connect with other nodes, it, at first, must solve a puzzle. An attacker does not likely have infinite resources and it is not possible for him to make connections fast enough to exhaust a serving node.

b. **DE synchronization**: Desynchronization refers to the disruption of an existing connection. In this attack, an attacker repeatedly forges messages to one or both points of an active connection and thus desynchronizes the end points so that the nodes retransmit messages and waste their energy.

One countermeasure against these attacks is to authenticate all packets exchanged between sensor nodes along with all the control fields in transport header [1].

Jellyfish attack: It is a one of the denials of service attack and a type of passive attack, which is hard to detect. This attack provides delay before the transmission and reception of data packets in the network. The Jellyfish attack, the malicious node can attack the traffic via itself by reordering packets, dropping packets periodically, or increasing jitters. The Jellyfish attack is particularly harmful to TCP traffic in that cooperative nodes can scarcely differentiate these attacks from the network congestion. The attack work against the TCP and UDP protocols, which are used for HTTP, FTP and video conferencing and disturb the performance of both protocols[1]. Jellyfish attack is similar to black hole but in jellyfish, an attacker node produces delay during forwarding packets. These attacks are targeted against closed loop flows.

7. CONCLUSION

This survey gives an idea of a major subset of security problems that a MANET faces because of its exceptional design characteristics. At the same time, this survey includes brief discussion on the important security aspects that are required to design a secure MANET. Some well-known attacks are discussed in this survey in order to give an idea about how the adversaries can actually attack the MANET, exploiting its vulnerabilities and what kind of security awareness should be taken into account when incorporating security mechanisms in MANET. There is no standard security mechanism that can provide overall security for MANET. Providing such a mechanism is very difficult. Designing a secure MANET needs proper mapping of security solutions or mechanisms with different security aspects. This also imposes a research challenge for MANET security.

REFERENCES

[1]. B. Wu, J. Chen, J. Wu, M. Cardei, "A Survey of Attacks and Countermeasures in Mobile Ad Hoc Networks," Department of Computer Science and Engineering, Florida Atlantic University.
http://student.fau.edu/jchen8/web/papers/SurveyBookchapter.pdf

[2].C.S.R.Murthy and B.S.Manoj, Ad Hoc wireless Networks, Pearson Education, 2008.

[3]. B.Wu, J.Chen, J.Wu, and M.Cardei, "A Survey of Attacks and Countermeasures in Mobile Ad Hoc Networks," Wireless/Mobile Network Security, Springer, vol. 17, 2006.

[4].H. Yang, H. Luo, F. Ye, S. Lu, L. Zhang, "Security in mobile ad hoc networks: challenges and solutions," In proc. IEE Wireless Communication, UCLA, Los Angeles, CA, USA; volume- 11, Page(s):38- 47, ISSN: 1536-1284

[5].M.A.Shurman, S.M.Yoo, and S.Park, "Black Hole Attack in Mobile Ad Hoc Networks," ACM Southeast Regional Conference, pp. 96-97, 2004.

[6].Y.C.Hu, A.Perrig, and D.Johnson, "Wormhole Attacks in Wireless Networks," IEEE Journal on Selected Areas in Communications, vol. 24, no. 2, pp. 370-380, February 2006.

[7].Sowmya P, V. Anitha, Defence Mechanism for SYBIL Attacks in MANETS using ABR Protocol, International Journal of Advanced Computer Research (ISSN (print): 2249-7277 ISSN (online): 2277-7970) Volume-4 Number-2 Issue-15 June-2014.

[8].A.Vani "A Study of Security Flaws and Attacks on AODV Routing Protocol" International Journal of Innovative Research in Computer and Communication Engineering, ISSN(Online): 2320-9801ISSN (Print) : 2320-9798, Vol. 3, Issue 6, June 2015,pp-5276-5280.

[9].Survey of Routing Attacks and Countermeasures in Mobile Ad Hoc Networks Amara korba Abdelaziz, Mehdi Nafaa, Ghanemi Salim Networks and Systems Laboratory University of Badji Mokhtar Annaba, Algeria - 2013 UKSim 15th International Conference on Computer Modelling and Simulation

[10].Hu YC, Perrig A, Johnson DV," Wormhole attacks in Wireless Networks", IEEE journal on selected areas in communications, 370-380, 2006.

[11].Magotra, Shikha, and Kush Kumar," Detection of HELLO flood attack on LEACH protocol", IEEE International Advance Computing Conference (IACC), 2014.

[12].F.H.Tesng.et.al, "A Survey Of Black Hole Attacks In Wireless Mobile Ad Hoc Networks", Human-centric Computing and Information Sciences, Vol.1, p.4,2011.(http://www.hcis-journal.com/content/1/1/4)