© 2016 IJSRSET | Volume 2 | Issue 2 | Print ISSN : 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

MANET : Services, Parameters, Applications, Attacks & Challenges

Sk. Heena Kauser*, P. Anil Kumar

Department of Computer Science & Engineering, PACE Institute of Technology & Sciences, Ongole,
Andhra Pradesh, India

ABSTRACT

Ad-hoc networks are the collection of autonomous nodes where all the nodes are configured dynamically without any centralized management system. Mobile Ad-hoc Networks (MANETs) are self-configuring network of mobile routers connected via a wireless link. A MANET is a most promising and rapidly growing technology and it have become a very popular research topic in recent years. This paper gives an overview of MANETs with respect to services, parameters, applications, attacks and challenges.

Keywords: MANET, Personal Area Network, Security Attacks

I. INTRODUCTION

Recent advances in computer networking have introduced a new technology for future wireless communication, a mobile ad hoc network (MANET). Ad hoc networks do not rely on any fixed infrastructure [5]. Instead, hosts rely on each other to keep the network connected. Each node in MANET can easily gain access to other nodes packets or inject fault packets to the network. Therefore, securing MANET against malicious behaviors and nodes became one of the most important challenges in MANET. The concept of security for (MANET) means protocols security to which you subscribe and deal with it in order to protect it from threats [1].

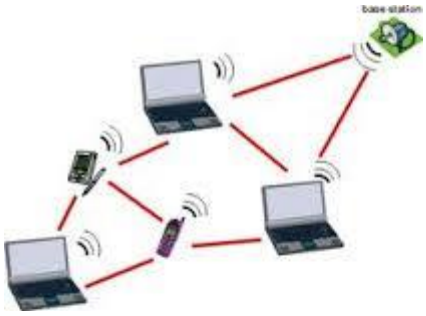

Figure1: MANET

In this paper, we present an elaborate view of services in MANET security. Based on MANET's special characteristics, we define three security parameters for MANET. The view of overall security attacks present in the Ad-hoc Networks till now. A comprehensive analysis in security challenges of MANET and solutions is presented.

II. METHODS AND MATERIAL

2. Security Services

The aim of a security service is to secure network before any attack happened and made it harder for a malicious node to breaks the security of the network. Providing these services faced lots of challenges. For securing MANET a trade-off between these services must be provided, which is depended on network application. We discuss five important security services and their challenges as follows:

2.1 Availability

Availability is to keep all the network resources available to genuine users where each authorized node must have access to all data and services in the network. It ensures the survivability of the network despite malicious incidents. Availability challenge arises due to MANET's dynamic topology and open boundary [2]. In the proposed approach which is called ABTMC (Availability Based Trust Model of Clusters), by using availability based trust model, aggressive nodes are identified quickly and should be isolated from the network in a period of time, therefore availability of MANET will be guaranteed.

2.2 Authentication

The goal of this service is the ability to verify a user's identity. When a node receives packets from a source, it must be sure about identity of the source node. One way to provide this service is by using certifications. Authentication is a fundamental mechanism to support access control [4].

2.3 Data Confidentially

Confidentiality ensures that the information transmitted over the network is unreadable to unauthorized users or nodes [4]. The basic idea is to transform a secret message into multiple shares by secret sharing schemes and then deliver the shares via multiple independent paths to the destination. Therefore, even if a small number of nodes that are used to transmit the message shares, been compromised, the secret message as a whole is not compromised. Using multipath delivering causes the variation of delay in packet delivery for different packets. It also leads to out-of-order packet delivery.

2.4 Integrity

According to integrity security service, just authorized nodes can create, edit or delete packets [2]. In this attack, all the packets are illegally modified or destroyed during transmission. Integrity is to be able to keep the data transmitted from being illegally modified or destroyed during the transmission.

2.5 Non-Repudiation

By using this service, neither source nor destination can reject their behavior or data. In other words, if a node receives a packet from node 2, and sends a reply, node 2 cannot repudiate the packet that it has been sent. All group members have a private key to ensure that another node couldn’t create packets with its properties.

3. Important Parameters in Manet Security

Because of MANET’s special characteristics, there are some important metrics in MANET security that are important in all security approaches; we call them “Security Parameters”. Security parameters in MANET are as follows:

3.1 Network Overhead

This parameter refers to how many number of control packets are generated. Due to shared wireless media, additional control packets may easily lead to congestion or collision in MANET. This results in loss of packet. Therefore, high packet overhead increases packet lost and the number of retransmitted packets. This will easily wastes nodes energy and networks resources.

3.2 Processing Time:

Each security approach needs time to detect misbehaviors and eliminate malicious nodes. Due to MANET’s dynamic topology it’s strongly possible that routes between two different nodes break because of mobility [2]. In order to avoid retransmission and increase flexibility processing time must be low.

3.3 Energy Consumption:

High energy consumption reduces nodes and network’s lifetime. In MANET nodes must have limited energy consumption because it is highly challengeable.

Each security protocol must be aware of these three important parameters. In some situations a trade-off between these parameters is provided in order to perform a satisfaction level in all of them. Security protocols that disregard these parameters aren’t efficient as they waste network resources.

4 MANET Applications

The set of applications for MANET is different, ranging from large-scale, mobile, highly dynamic networks, to small, static networks that are controlled by power sources.

Typical applications include-

4.1 Military Battlefield

Now a days military contains some sort of computer equipments. Ad- hoc networking would allow the military to take advantage of commonplace network technology to maintain an information network between the soldiers, vehicles, and military information headquarters [7]. The basic techniques of ad hoc network came from this field.

4.2. Commercial Sector

Ad hoc can be used in emergency operations for disaster relief efforts, e.g. in fire, flood, or earthquake [7]. Emergency operations must take place where rapid deployment of a communication network is needed. Information is transmitted from one team member to another over a small hand held.

4.3. Local Level

Ad hoc networks can separately link a temporary multimedia network using notebook computers or laptop computers to spread and share information among participants. e.g. at conference or classroom. Another local level application might be in home networks where devices can directly exchange information. Similarly in other environments like taxicab, sports stadium, boat and small aircraft…etc

4.4. Personal Area Network (PAN)

Short-range MANET can simplify the intercommunication between various mobile devices (such as a PDA, a laptop, and a cellular phone [7]. Wired cables are replaced with wireless connections. It also extends the access to the Internet by Wireless LAN (WLAN), GPRS, and UMTS.

5. Security Attacks in MANETS

Mobile Ad hoc networks are vulnerable to various attacks not only from outside but also from within the network itself. Ad hoc network are mainly subjected to two different levels of attacks [4]. The first level of attack occurs on the basic mechanisms of the ad hoc network such as routing. Whereas the second level of attacks tries to damage the security mechanisms employed in the network.

The attacks in MANETs are divided into two major types.

A. **Internal Attacks**
   Internal attacks are directly leads to the attacks on nodes presents in network and links interface between them. This type of attacks may broadcast wrong type of routing information to other nodes. Internal attacks are sometimes more difficult to handle as compare to external attacks, because internal attacks occurs due more trusted nodes[4].

B. **External Attacks**
   These types of attacks try to cause congestion in the network, denial of services (DoS), and advertising wrong routing information etc. External attacks prevent the network from normal communication and producing additional overhead to the network. External attacks can classify into two categories:

Passive Attacks
Active attacks

5.1. Passive Attacks

MANETs are more susceptible to passive attacks. A passive attack does not alter the data transmitted within the network. Passive attacks are started by attackers to steal useful information from the targeted networks [8]. Table 1 summarizes the passive attacks in MANET. The attackers do not otherwise need to communicate with the network. Passive attacker does not disrupt the operation of a routing protocol but attempts to discover the important information from routed traffic for future harmful attacks [4].

Table 1. Passive Attacks

Reference	Attack	Effects
[6]	Eavesdropping	Eavesdropping is a passive attack, which occurred within the mobile ad-hoc network. The aim of eavesdropping is to find some secret or confidential information that should be kept

		secret during the communication.
[1]	Traffic Analysis	It is based on the track and analysis of the flow of traffic so as to know the network scheme, leading to detect nodes and have access to them.
[1]	Monitoring	It is based on access to confidential data without being able to change or amend them.
[3]	Replay attack	It includes replay of previously captured routing traffic by the malicious node. It is done to create erroneous routing information and misleading the network.

5.2. Active Attacks

Active attacks are very severe attacks on the network that prevent message flow between the nodes. However active attacks can be internal or external. Active external attacks can be carried out by outside sources that do not belong to the network. Table 2 summarizes the active attacks in MANET. Internal attacks are from malicious nodes which are part of the network, internal attacks are more severe and hard to detect than external attacks.

Table 2. Active Attacks

References	**Attacks**	**effects**
[2]	Snooping attack	The goal of this attack is accessing to other nodes packets without permission. As in MANET packets transmitted hop by hop, any malicious node can capture others packets
[2]	Fabrication Attack:	In fabrication attack, malicious node destroys routing table of nodes by injecting fault information. Malicious node creates fault routing paths. As a result, nodes send their packets in fault routes.
[6][10]	Worm Hole Attack	In wormhole attack, The attacker nodes present in the network at one side captures the packet from the legitimate node and encapsulates the packet with the help of tunnel and transmit it to the other attacker node or malicious node present in the network.
[2]	Denial of service	In this attack, malicious node prevents other authorized nodes to access network data or services. Using this attack, a specific node or service will be inaccessible and packet delay and congestion increases.
[3]	Black Hole Attack	In these attacks, the malicious node keep on sending positive replies for the route requests it is getting,inspite of the fact that whether the related routes are available or not. Ultimately, drops all the packets that are routed to its destination via this node.
[1]	Byzantine attack	It consists of a set of nodes and is collectively sets up guide rings, and it also guides packets in worst tracks.
[4][9]	Sinkhole attack	The compromised node advertises itself in such a way that it has shortest path to the destination. Malicious node than capture important routing

		information and uses it for further attacks such as dropping and selective forwarding attacks.
[6]	Rushing attack	In rushing attack, an attacker comes between the route of sender and receiver. When sender send packet to the Receiver, then attacker captures the packet and forward to receiver. Attacker then sends the duplicate packet to the receiver again and again. Then Receiver assumes that packets come from sender.

III. RESULTS AND DISCUSSION

Challenges In Manet Network

The challenges facing the (mobile ad hoc) networks are a concern for the design and communication processes in the network. There are different security challenges in MANET namely:

- **Mediums of Wireless Communication**

By nature the MANET network is a wireless network. Signals are transmitted between network nodes through a joint medium. The wireless medium is considered extensive and unrestricted with any limits of any open centre. Broadcast Wireless using medium allows easy message Eavesdropping and Injection [8].

- **Infrastructure and Routing:**

The basis of the work of network is independent of any infrastructure, and this leads to any viable classic list of the application on the certification and on servers line [1]. The nodes in the network are constantly moving, changing the nodes from time to time and this makes it difficult to predict the patterns of distribution and dealing with route decisions.

- **Energy Consumption**

The cellular phones that subscribe in (MANET) network rely on energy sources such as batteries, which is a problem in wireless networks. A device in (MANET) works as a director which constantly communicates with other devices, and this energy plays an important role [1].

- **Scalability**

The MANET network is expandable and scalable in terms of the number of nodes and topology. The size of the network and the number of nodes connected to the network plays an important role in control mechanism. Therefore, the network must be provided, regardless of the size and number of nodes in the network.

- **Bandwidth**

Bandwidth in MANET network is regarded a difficult problem, because it is shared between the neighboring hosts, while individual host has no knowledge about the other traffic of the neighboring hosts. In MANET network the routing tables of nodes are updated repeatedly and continuously, and this leads to the consumption of a large amount of bandwidth.

- **Software and Applications in Devices**

Developed devices in MANET are used to access e-mail, various applications and data, games, etc. The Social networking programs contain user information and are used to communicate with others without restrictions and control.

IV. CONCLUSION

In this paper we introduce MANET, services, parameters, challenges in security and Attacks on MANETs. The MANET network, like other networks, faces some of the challenges that have been studied in this paper and we discussed five important security services and three important security parameters. We have also kept a close look on the attacks and have tried to bind the attacks into categories. With the passage of time challenges are renewed and security attacks are renewed corresponding with the developments.

V. REFERENCES

[1] Dr.Nabeel Zanoon1, Dr.Nashat Albdour2, Dr.Hatem S. A. Hamatta1, and RashaMoh'd Al-Tarawneh1, “SECURITY CHALLENGES AS A FACTOR AFFECTING THE SECURITY OF MANET: ATTACKS, AND SECURITY SOLUTIONS”, International Journal of Network Security & Its Applications (IJNSA) Vol.7, No.3, May 2015, pp. 1-13.

[2] Ali Dorri and Seyed Reza Kamel and Esmail kheyrkhah, Department of Computer Engineering, Mashhad branch, Islamic Azad University, Mashhad, Iran.“SECURITY CHALLENGES IN MOBILE AD HOC NETWORKS: A SURVEY” International Journal of Computer Science & Engineering Survey (IJCSES) Vol.6, No.1, February 2015, pp.15-29.

[3] Ms.Supriya1 and Mrs.Manju Khari2, “MANET SECURITY BREACHES :THREAT TO A SECURE COMMUNICATION PLATFORM”, International Journal on AdHoc Networking Systems (IJANS) Vol. 2, No. 2, April 2012, pp.45-51.

[4] T. Navaneethan, M.Lalli,”Security Attacks in Mobile Ad-hoc Networks – A Literature Survey”, T.Navaneethan et al, International Journal of Computer Science and Mobile Applications, Vol.2 Issue. 4, April- 2014, pg. 1-7.

[5] Sarvesh Tanwar, Prema K.V. “Threats & Security Issues in Ad hoc network: A Survey Report”, International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-6, January 2013, pp.138-143.

[6] Aarti Chauhan, Puneet Rani. “A Detail Review of Routing Attacks in Mobile Ad Hoc Networks”, International Journal of Engineering Research and General Science Volume 3, Issue 2, March-April, 2015 ISSN 2091-2730 , pp.1154-1163.

[7] Mr. Vikas Kumar, Mr. Amit Tyagi, Mr. Amit Kumar. “Mobile Ad-hoc Network: Characteristics, Applications, Security Issues, Challenges and Attacks”, Volume 5, Issue 1, January 2015 ISSN: 2277 128X, International Journal of Advanced Research in Computer Science and Software Engineering, pp.258-262.

[8] ”A REVIEW: TRUST, ATTACKS AND SECURITY CHALLENGES IN MANET”, Informatics Engineering, an International Journal (IEIJ), Vol.3, No.3, September 2015, pp.293-298.

[9] Rama Chaithanya Tanguturi & Jayakuamar C 2015, 'Agent based security framework towards misrouting attack in wireless sensor networks', International Journal of Scientific Research in Science, Engineering and Technology, vol. 1, no. 4, pp. 203-206.

[10] M. V. Bharathi, R. C. Tanguturi, C. Jayakumar and K. Selvamani, "Node capture attack in Wireless Sensor Network: A survey," Computational Intelligence & Computing Research (ICCIC), 2012 IEEE International Conference on, Coimbatore, 2012, pp. 1-3.