MANET: Security Aspects and Challenges

Md Tanzilur Rahman[#1], Kunal Gupta[*2]

Computer Science Department, Amity University
Sec-125, NOIDA, Uttar Pradesh, INDIA

Abstract **– There have been a huge advancement in the field of wireless networks in last few decades. It gives new direction in the field of internet with its large number of applications. A mobile ad hoc network or MANET is self-configuring infrastructure less network of mobile device (laptops, smartphones, sensors, etc.) connects by wireless link. This type of network is standalone network. Security is a primary issue in order to provide secure communication in hostile environment. There are still some challenges associated with MANETS that needs to be overcome. These challenges includes routing, short battery life, limited capacity, dynamically change topology etc. In this paper we present the fundamental challenging issues, Security challenges and different types of Attacks associated with MANETs.**

Keywords: **MANETs, Ad Hoc Networks, Routing protocols**

I. INTRODUCTION

MANET is a new generation technology which allows its user to communicate without any fixes infrastructure without taking into consideration its geographical location [4]. A fixed supporting structure limits the adaptability of wireless system. In infrastructure wireless networks, a user directly communicates with an access point or base station but on the other hand MANET, never rely on a fixed infrastructure for its operation, a MANET is a self-configuring infrastructure less network of mobile devices connected by wireless. The mobile devices or the nodes of the MANTES are free to move, enter and leave overtime, node also can act as a router that can forward packets due to lack of infrastructure support. Ad hoc network also allows to device to maintain connection to the network as well as easily removal and add up of devices. Due to this node mobility feature the topology of the network changes dynamically, hence the network is decentralized. Due to mobility of nodes MANETS are more vulnerable than wired networks in many scenarios.

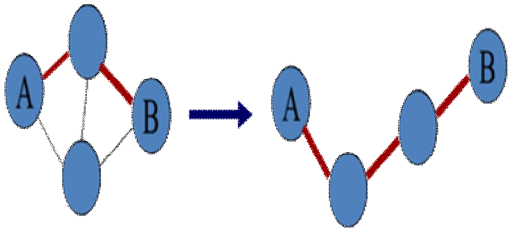

Figure A: Topology change frequently

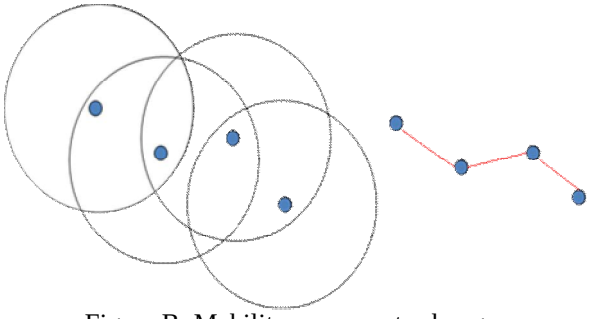

Figure B: Mobility cause route changes

II. WHY AD-HOC NETWORK

As we know that in many of the cases it is not always possible and feasible to set up a fixed access point and backbone infrastructure because infrastructure may not be present disaster area or war zone as in such areas is impossible to lay down wires or provide infrastructure network services as well as infrastructure may not be practical for short range radios as Bluetooth (range 10m).

But if we talk about ad hoc network it does not need fixed infrastructure hence can easily be deployed and proved to be very useful where infrastructure is absent, destroyed or impractical such as in war zone and disaster area.

A) *FEATURES*

- **Autonomous terminal**: A node may function as both host and a router.
- **Distributed Operations:** since there is no fixed network the control and management operations are distributed among the terminals.
- **Multi-hop routing**: packets should be delivered via one or more nodes.
- **Dynamic network topology:** As the network change rapidly, the mobile nodes dynamically establish routing among themselves i.e. they form their own network
- **Fluctuating link capacity:** One end-to-end path can be shared by several sessions.
- **Light-weight terminal:** The MANET nodes are mobile devices with less CPU processing capability, small memory size, and low power storage.

B) ISSUES

As we have mentioned earlier MANET is more vulnerable than wired network. Some of the vulnerabilities are mentioned below:

- **No centralized management**: Lack of centralized management make it very difficult to detect the attacks because it is very difficult to analyse traffic in highly dynamic and large scale ad hoc network
- **Absence of infrastructure:** Ad hoc network works without having any fixed infrastructure and makes inapplicable any classical solution based on certification authorities and online servers.
- **Limited power supply:** Due to nodal mobility in ad hoc network the nodes will rely on the battery for their power supply and provided by limited power supply that will result in many problems DOS attack and selfish manner.
- **Dynamic network topology:** Ad hoc network allow the nodes to move frequently hence the network topology may change randomly in an unpredictable manner. This dynamic behaviour of the nodes also disrupts the nodes relationship. Dynamic behaviour can be protected in better manner with the help of distributed and adaptive security mechanism.
- **Bandwidth constraint:** Nodes used by the MANETs has a wide range of capacity and in general wireless bandwidth is more error prone as well as insecure also than that of wired. These factors lead to lower capacity throughput than equivalent wired links. These lower capacity wireless link lead to the more congestion problems.
- **Limited physical security:** Mobile wireless links have comparatively more error prone and have more security threats than hardwired networks. Hence this results into increased possibility of DOS attacks and spoofing.
- **Variable capacity nodes:** Nodes may have one or more interfaces of varying transmission capacity that can operate on different frequency band. This radio capability of node may result in asymmetric links.

III. MANET security

A major issue in mobile ad hoc network is security. The goals of security mechanism in MANET are similar to that of other networks. Security is one of the main concerns in the network specially where security attacks can affect the nodes limited resource. There are two approaches in protecting mobile ad hoc network

- **Reactive approach:** Seeks to detect security threats and react accordingly.
- **Proactive approach:** Attempts to prevent an attacker from launching attacks through various cryptographic techniques

A) Issues in securing MANETs

- **Secure multicasting:** Is a communication method where a single data packet can be transmitted from a sender and replicated to a set of receivers.
- **Secure routing:** Most MANET routing protocols are vulnerable to attacks that can freeze the whole network. Need some solutions that work even if some nodes compromised**.**
- **Privacy-aware Routing**: Building routing protocols that prevent intermediate nodes from performing traffic analysis and Schemes for minimizing size of crypto-tags(digital signatures) are needed.
- **Key Management**: security goals in MANET are mainly achieved through trusted Certificate Authority (CA) hence compromised CA can easily damage the entire network.
- **Intrusion detection and response schemes:** Anomaly detection is difficult in MANETs (ex: types of attacks and their source). Collaborative IDS schemes are needed for the same.

B) Security goals

- **Authentication:** A node must know the identity of the peer node it is communicating with. Without

authentication, an attacker could gain sensitive information and interfere with other nodes.

- **Confidentiality:** confidentiality ensures that the assets of the computer are only accessed by authorized use. It concentrates on the fact that information is never disclosed to unauthorized entities.
- **Integrity:** The goal of integrity is that assets can only be modified by authorized user. It Guarantees that Message being transmitted is never corrupted.
- **Availability:** Nodes should be available for communication at all times. A node need continue to provide services despite attacks. E.g.: Key management service.
- **Non-Repudiation:** The sender cannot later deny sending the information and the receiver cannot deny the reception of information.
- **Authorization:** Provide different access rights to different type of users. For example a network management can be performed by network administrator only.
- **Detection and Isolation:** Require the protocol can identify misbehaving nodes and render them unable to interfere with routing.

IV. MANETs Security attacks

Securing wireless ad hoc network is highly challenging task. The attacks on Manets are studied in many past literatures previously [1, 3]. The main concern is the secure communication in MANETs and therefore secure transmission of information is necessary. MANETs are more vulnerable than that of wired network hence is more threatened by the security attacks. These attacks can be classified as

Active attack: The ultimate goal of Active attack is to alter or destroy the data that is being transmitted. It can harm the network operation or some nodes in different ways such as by inserting his own data into data stream, deletion of data etc. Active attack can be classified in two categories, attacks done by the nodes that do not belong to the network is called external attack and another one is internal attack which is carried out by the nodes that actually the part of the network.

Passive attack: A passive attack does not disrupt proper operation of the network it only reads/snoops the data being transmitted. A malicious node either ignores operations supposed to be accomplished by it in passive attack

Denial of service attack: The target of this type of attack is availability of nodes or the entire network. Malicious node floods irrelevant data to consume network bandwidth or to consume the resources (e.g. power, storage capacity or computation resource) of a particular node. If they succeed in their target the services will not be available.

Tunnelling/Wormhole attack: Tunnelling Attack is also known as wormhole attack. In wormhole attack an attacker receives a packet at one point of network and tunnels them to another point of the network and reply back to them from that point of the network. This is called tunnelling attack because the colluding malicious nodes are linked through a private network connection which is invisible at higher layers. This tunnel between two colluding attacks is known as a wormhole. Routing can be disturbed when routing control message are tunnelled.

Black hole attack: In this type of attack the attacking node provides the fake routing information such that it has optimum path, causing source node to choose a path through that particular node so that the attacker can then misuse or drop messages as it sees fit.

Reply attack: In reply attack a valid data is r fraudulently repeated or delayed. Attacker records another nodes control messages and resends them later. Can be used to spoof another node or just disrupt routing.

Byzantine Attack: Compromised intermediate nodes works alone or set of compromised intermediated nodes works in collusion and carry out attacks. These attacker nodes create routing loops, forwarding packets through non-optimal path or selectively dropping packets which cause the disruption or degradation of routing services.

Routing attacks: There are several attacks that can affect routing to a large extend such as routing table overflow, routing table poisoning, packet replication, route cache poisoning and rushing attack.

Sybil attack: Sybil attack attempts to degrade the integrity of data, security and resource utilization that the distributed algorithm tries to achieve. Sybil attack can be performed for storage, routing mechanism, air resource allocation and misbehaviour detection. Basically, any peer-to peer network (especially wireless ad hoc networks) is vulnerable to Sybil attack.

Layer	Attacks
Application Layer	Repudiation, Data corruption.
Transport layer	Session hijacking, SYN flooding
Network Layer	Wormhole, Blackhole, Byzantine, Flooding, Resource consumption, Location disclosure attacks.
Data Link Layer	Traffic analysis, Monitoring , WEP weakness
Physical Layer	Jamming, Interception, Eavesdropping
Multi Layer Attack	Dos, Replay, Man in the Middle, Impersonation

Figure C: Security Attack on protocol stack

V. MANET Applications

Ad-hoc networking is gaining much more importance due to its wide range of applications because huge number of huge number of portable devices as well as the popularity of wireless communication. Ad-hoc networking is applicable anywhere such as the place where little or no communication infrastructure is possible because it doesn't have a predetermined infrastructure. Some of the typical applications are mentioned below [8][12]

Military services: MANETS can be used for automated battle fields, technical networks as well as for military communication. It allows to have a information network between soldiers military vehicles and their head quarters with the help of small hand held devices.

Disaster relief: The infrastructure of the networks are almost destroyed or completely damaged due to natural calamity. So in case of disaster we need such a network that can easily be deployed in such reasons and can provide emergency services for the purpose of relief. Ad-hoc network can be used easily in disaster relief such as fire, flood or earthquake to overcome the problems of damaged infrastructure occurred by the natural calamity.

Sensor Networks: It can also be used as Wireless sensor networks since it consist of the devices having the capability of computation, sensing as well the capacity of wireless networking. In wireless sensor networks the capability of smoke detectors, electricity, water and gas meters are combined to perform such tasks efficiently [9]. It can also be used as data networks since MANET provide support to the network for data exchange between mobile devices [9].

Personal Area Networking: Intercommunication between various mobile devices such as laptop and cell phone etc are also provided by short range of MANET. The services like internet and GPRS are also gaining the popularity due to MANET.

VI. Conclusion and future scope

Since MANET are future network as it is easy to deploy practically versatile and comparatively inexpensive so its future is highly appealing that provide us "all time, all situation" cheapest communication. Mobile ad hoc networks have the ability to set up network and provide communication in such an environment where it is really impossible to have a traditional infrastructure network. The research on MANET and its security is still in its early stage, there are lots of technical issues that needs to be answered [10]. Improvement in bandwidth and capacity is required which need better spectral reuse and better frequency also. Due to mobility and open media nature MANET is easily vulnerable to security than that of other wired networks. So MANET requires better security mechanism in order to provide secure communication than wired networks. Research in the field of security is still open, , we can design a security mechanism by which we can minimize or can completely remove many of those threats and attacks.

VII. References

[1] Hoang Lan Nguyen, Uyen Trang Nguyen. "A study of different types of attacks on multicast in mobile ad hoc networks". Ad Hoc Networks, Volume 6, Issue 1, Pages 32-46, January 2008.

[2] Humayun Bakht "History of Mobile Ad hoc Networks" http://www.oocities.org/humayunbakht/HMANET.pdf

[3] Nishu Garg, R.P.Mahapatra. "MANET Security Issues". IJCSNS International Journal of Computer Science and Network Security, Volume.9, No.8, 2009.

[4] Jeoren Hoebeke, Ingrid Moerman, Bart Dhoedt and Piet Demester "An Overview of Mobile ad hoc Netwroks: Applications & Challenges ."

[5] Bin Xie and Anup Kumar. "A Framework for Internet and Ad hoc Network Security". IEEE Symposium on Computers and Communications (ISCC-2004), June 2004.

[6] Ram Ramanathan and Jason Redi "A Brief Overview Of Ad Hoc Networks: Challenges and Directions" IEEE Communications Magazine-50th Anniversary Commemorative Issue/May 2002

[7] Y.Hu, A Perrig and D. Johnson, Ariadne: A secure On-demand Routing Protocol for Ad Hoc Networks, in Proceeding of ACM MOBICOM'02, 2002.

[8] HaoYang, Haiyun & Fan Ye — Security in mobile ad-hoc networks : Challenges and solutions,‖, Pg. 38-47, Vol 11, issue 1, Feb 2004.

[9] Andrea Goldsmith "Wireless Communications" Cambridge University Press.

[10] Pravin Ghosekar, Girish Katkar, Dr. Pradip Ghorpade "Mobile Ad Hoc Networking: Imperatives and Challenges"

[11] A Mishra and K.M Nadkarni, security in wireless Ad -hoc network, in Book. The Hand book of Ad Hoc Wireless Networks (chapter 30), CRC press LLC, 2003.

[12] M. Frodigh, P. Johansson, and P. Larsson.—Wireless ad hoc networking: the art of networking without a network,‖ Ericsson Review,No.4, 2000, pp. 248-263.