A Study on MANET and its Security Concepts

Author 1: **J.Viba Mary**
Asst. Professor, Dept. of Software Systems,
KG College of arts & science,
Bharathiar University, Coimbatore, India-641035
Phone no - 9500896380
vibamphil@gmail.com

Author 2: **K.Gomathi**
Asst. Professor, Dept. of Software Systems,
KG College of arts & science,
Bharathiar University, Coimbatore, India-641035
gomathisfcw@gmail.com
Phone no – 8870856581

ABSTRACT: The Computer Network technology is developing rapidly and the recent advances have introduced a new technology for wireless communication over the internet in future in MANET. It becomes the popular research topic in recent years. Security has become one of the most important challenges against malicious behaviours and nodes in MANET and there are more studies focused on several security problems. After quantifying and analysing the network information Security elements like integrity, availability and confidentiality, we are going to discuss about the overview of security issues in detail with respect to services, parameters, applications, attacks and challenges, some of the applications that is used in MANET and also the various types of attacks that can be involved internally as well as externally such as delay of packets, time consumption and bandwidth etc.,

KEYWORDS: Security Issues, Network Security, MANET, Security Elements

I. INTRODUCTION

Mobile Ad Hoc network is a collection of nodes or communication devices. It does not rely on any fixed infrastructure and pre-determined organization of available links. The host that available in the Ad Hoc network rely on each other to keep the network connected. That is how MANET has become the revolutionary challenge in the computing world. It is a set if wireless mobile hosts dynamically establish their own network without relying on any pre-existing communication infrastructure. But these kinds of dynamic network topology are prone to be attacked externally as well as internally. Here we are going to discuss about the security issues, security attacks & goal of the security solutions to provide the various kinds of security services for MANET [5].

The main study of this paper is how to prevent the network from the various types of attacks that can easily interrupt the nodes. The rest of the paper is organized as follows, Section I contains the introduction of MANET, Section II contain the related work of security attacks in MANET, Section III contain the some applications of MANET, Section IV explain the methodology and measures of preventing MANET, Section V describes results and discussion, Section VI concludes research work with future directions).

II. SECURITY ATTACKS IN MANET

Understanding possible form of attacks is always the first step towards developing good security solutions. It is important for secure transmission of information. There are some basic class of attacks in MANET that can cause slow network performance, delay of messages, uncontrolled traffic, etc. Attacks can be categories into four types.

- **Internal Attack:** In an internal attack, the malicious node in the same network gains the unauthorized access and impersonates as a genuine. It also participates in other network activities and analyses the traffic between other nodes.
- **External Attack:** In an external attack, the malicious node from other network gains the unauthorized access and causes congestion sends false routing information or causes unavailability of services [5].
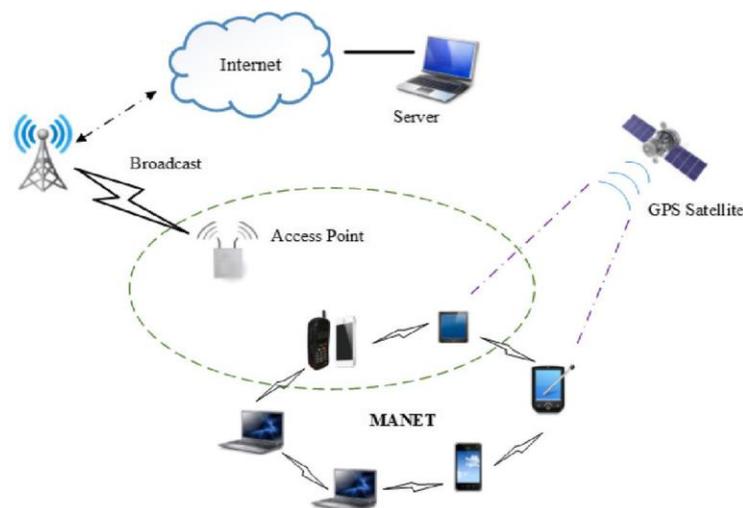

Figure 1: MANET Network Topology

- **Active Attack:** In an active attack, the malicious node from any network takes control of a communication between two entities and masquerades as one of them jamming, which causes channel unavailability by overusing it[6].
- **Passive Attack:** In a passive attack, the malicious node from any network, the attacker eavesdrops packets and analyses them to pick up required information [6].

Table 1 : Difference between Active & Passive attacks

Active Attack	Passive Attack
Access and modify information	Access information
System is harmed	No harm to system
Threat to integrity and availability	Threat to confidentiality
Easy to detect than prevent	Difficult to detect than prevent
Dos, Repudiation, Masquerading	Traffic analysis, Snooping

III. MANET APPLICATIONS

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

- **Commercial Sector:** Emergency operations must take place where rapid deployment of a communication network is needed. It is used in emergency operations for disaster relief efforts, e.g. in flood, fire or earthquake [1].
- **Military Battlefield:** MANET allows the military to take advantage of common place network between the vehicles, soldiers and military information headquarters [1].
- **Local Level:** Ad Hoc networks can link a temporary multimedia network using separately using notebook computers or laptop computers to spread and share information among participants like conference hall or classroom [1].

IV. METHODS AND MATERIALS

IV.I Security goals for MANET

All networking functions such as packet forwarding and routing, are performed by node themselves in a self-organizing manner. So securing a Mobile Ad Hoc network is very challenging. The goals to evaluate if Mobile Ad Hoc network is secure or not are as follows [2]:

IV.II Confidentiality

Confidentiality refers to protecting information from being accessed by unauthorized parties. In other words, only the people who are authorized to do so can gain access to sensitive data. To maintain confidentiality, we need to keep them secret from all entities that do not have the privilege to access them.

IV.III Integrity

Integrity refers to ensuring the authenticity of information that information is not altered, and that the source of the information is genuine. It guarantees the identity of the messages when they get transmitted and can be compromised mainly in two ways:

- Malicious altering
- Accidental altering

IV.IV Availability

Availability means that information is accessible by authorized users. This security issue is challenged mainly during the denial of service attacks, in which all the nodes in the network can be attack target and some selfish nodes make some network services unavailable, like routing protocol or the key management service.

Figure 2: Security Goals

V. RESULTS AND DISCUSSION

Challenges in MANET Network

The challenges facing the Mobile Ad Hoc networks are a concern for the communication processes and the design in the network. There are different security challenges in MANET namely:

- **Energy Consumption:** The mobile phones in Mobile Ad Hoc network relies on energy sources such as batteries, which is a problem in wireless networks. The energy source of a device in this network plays an important role because it constantly communicates with other devices[3].

- **Scalability:** The network must provide the regardless of the size and number of nodes in the network. The scalability of this network plays an important role in control mechanism. Thus the MANET is expandable and scalable in terms of number of nodes and topology.

- **Bandwidth:** The routing tables of nodes are updated repeatedly and continuously, and it leads to the consumption of a large number of bandwidth[7]. To maximize the overall network lifetime, we need a path with the maximal remaining power after data transmission. With the link bandwidth and the desired amount of data transmitted, the consumption power is computed to obtain the remaining power of a mobile node.

- **Software and Applications in Devices:** The Social networking programs contain user information and are used to communicate with other without any limitations or restrictions. Developed devices in MANET are used to access e-mail, various applications and data, games, etc.

- **Medium of Wireless Communication:** The 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. The broadcast Wireless using medium allows easy message Eavesdropping and Injection [4].

VI. CONCLUSION

In MANET, the node looks like selfishness. A node can use the resources of other node and preserve the resources of own. These types of nodes create many problems in the network. There are many numbers of ways, which can guarantee for the safety and security of your network. In this paper we discussed about the security issues, attacks, and challenges. Like other network MANET also faces some of the challenges that have been studied in this paper. With the passage of time challenges are renewed and security attacks are renewed corresponding with the developments. This paper concludes that to overcome these kinds of attacks and issue, we have to focus deeply on several security problems and the countermeasures to be taken against these problems in MANET.

REFERENCES

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

[2]. Sachin Lalar. Security in MANET: Vulnerabilities, Attacks & Solution. International Journal of Multidisciplinary and Current Research: January 2014; Volume 2.

[3]. Dr. Nabeel Zanoon, Dr.Nashat Albdour, Dr. Hatem, et al. Security Challenges as a Factor Affecting the Security of Manet: Attacks and Security Solutions. International Journal of Network Security & its Applications (IJNSA); May 2015; Volume 7; No.3; pp. 1-13.

[4]. Ashish Kumar Khare et al. A Review: Trust, Attacks and Security Challenges in Manet. Informatics Engineering, an International Journal (IEIJ); September 2015; Volume 3; No.3; pp. 293-298.

[5]. P.Anil Kumar and Sk.Heena Kauser. Manet: Services, Parameters, Applications, Attacks & Challenges. International Journal of Scientific Research in Science, Engineering and Technology; March 2016; ISSN: 2395-1990; Volume 2; Issue 2.

[6]. Mohan V.Pawar, Anuradha.J. Network Security & Types of Attacks in Network. International Conference on Computer, Communication and Convergence; May-2015; Volume 3; pp.503-506.

[7]. Ajitha.P, Chandra.E. Constructing Scalable local Distributed Decision Trees algorithm for heterogeneous data sources. International Journal on Computer Science and Engineering; Volume 3; Issue 1; pp-262-265.

[8]. A.Vani. Detection and Elimination of Wormhole Attacks in MANET. International Journal of Scientific Research in Computer Science & Engineering; October 2017;Volume 5; Issue 5; pp.35-40.