https://dx.doi.org/10.24001/ijaems.3.2.11 *ISSN: 2454-1311*

An Overview of Wireless Local Area Networks and Security System

Moumita Basak, Prof. Siladitya Sen

Department of Electronics and Communication Engineering, Heritage Institute of Technology, Kolkata, India

Abstract— *Wireless Communication is one of the fastest growing technologies in the world which is an application of technology and science in the modern life. Radio and telephone to current devices such as mobile phone, laptops, television broadcasting are the most essential part of our life. Wireless LAN, Cellular Telephony and Satellite based communication networks are the several parts of the wireless communication industry. In this paper, we have emphasized on a study of Wireless LAN technologies and its concerned issues: Wireless Networking, What WLANs are, History of WLAN, Need of WLAN, Types of WLAN, Advantages of WLAN, IEEE 802.11 Standards, Network Security.*

Keywords— WLAN, IEEE 802.11 Standard, some risks and attacks, Network Security.

I. INTRODUCTION

Wireless Local Area Network: A Wireless LAN is a wireless computer network that connects two or more devices using radio frequency channels as their physical medium within a limited area, such as home, office, school, computer laboratory etc. WLANs are the popularly increasing wireless networks which provide the network services without connecting with wires or cables is very difficult and too expensive to lay cabling for a wireless network.

Access points and Network interface cards are two basic components of WLAN. The stationary nodes are called Access Point which concerns with coordination of communication between the nodes and exchange the information by means of antenna in the WLAN. In a WLAN, Access Points can transmit and receive data. A Network Interface card scans available frequency spectrum from the environment and normally connects a wireless station to the access point in the Wireless LAN.

II. HISTORY OF WIRELESS LOCAL AREA NETWORK

Guglielmo Marconi invented the world's first wireless radio communication system in 1897. In 1901, he successfully demonstrated his wireless telegraph system to the world by transmitting radio signals across the Atlantic Ocean from England to America, covering more than 1,700 miles [1].

In 1971 world's first wireless computer communication network was developed by Norman Ambramson, professor at University of Hawaii. Costly hardware part of WLAN was replaced by various versions of IEEE 802.11 Standards at the end of the 1990's. At the beginning of 1991, HYPERLAN/1 was pursued and was approved in 1996.

In the year of 2000, HYPERLAN/2 was approved. IEEE 802.11n was invented and added to the IEEE 802.11 Standard which operates in both 2.4 GHz and 5 GHz.

III. REQIREMENTS OF WLAN

The medium access control protocol should be as efficient as possible which can maximize the throughput.

- Hundreds of nodes should be needed.
- Service area of WLAN is 100 to 300m.
- Battery power consumption should be less in sleep mode.
- WLAN provides secured license free operation.
- Reliable transmission and security is provided.
- Desired Quality of Service is required.

IV. TYPES OF WLAN

There are three types of WLANs-

➢ **Infrared (IR) LANs-**

- Infrared LANs are basically used at home for various remote control devices.
- It is bounded in a single room because it cannot penetrate the opaque walls.
- These LANs are inexpensive and simple to design.

➢ **Spread Spectrum LANs-**

- Topology can be either hub or peer to peer.
- It operates in ISM (Industrial, Scientific and Medical) bands.
- The major function of hub is automatic handoff of mobile stations.
- FCC licensing is not required.

➢ **Narrowband microwave-**

- These types of LANs can operate at microwave frequencies and do not use spread spectrum.
- It needs FCC licensing for some products.

V. ADVANTAGES OF WLAN

- Flexibility and mobility is greater advantage of WLAN.

https://dx.doi.org/10.24001/ijaems.3.2.11 *ISSN: 2454-1311*

- WLANs are very easy to install because there is no need of cable or wire connection.
- Portability is another advantage of WLAN.
- Maintenance cost is less. So it is less expensive.

VI. IEEE 802.11 STANDARDS

IEEE 802.11 Standard was developed and released by IEEE group for Wireless Local Area Networking in the year of 1997 (Cisco Wireless LAN standard report, 2000). Initially this standard specifies 2.4 GHz operating frequency, defining 1 Mbps and 2 Mbps speeds. IEEE 802.11 standard focuses on two layers of OSI Model- Physical Layer and MAC Layer. In September 1999, IEEE added two initial 802.11 Standard- Highly Scalable WLAN 802.11a which operates in the 5 GHz band at data rates up to 54 Mbps and 802.11b included two higher speeds (5.5 and 11 Mbps) to 802.11. IEEE 802.11g also operates at the 2.4 GHz ISM (Industrial, Scientific and Medical) band at data rates up to 54 Mbps.

IEEE 802.11 standard support two modes of WLAN-

- **Ad Hoc mode**- It supports peer to peer connection. Access point is not required. Full mesh or partial mesh topology is built.
- **Infrastructure mode**- In this mode of operation at least one access point is needed to communicate between two nodes.

IEEE 802.11 supports three physical layer specifications for wireless local area network: Diffused Infrared (IR), Frequency Hopping Spread Spectrum (FHSS), Direct Sequence Spread Spectrum (DSSS) where Infrared operates at the 5 GHz band and other two operate at the ISM (Industrial, scientific and medical) band 2.4 GHz.

Table.1: IEEE 802.11a, 802.11b, 802.11g standards

	IEEE 802.11a	IEEE 802.11b	IEEE 802.11g
Standard Ratified	Sep. 99	Sep 99	May 2003
Raw Data Rates	54 Mbps	11 Mbps	54 Mbps
Average Actual Throughput	**4-5 Mbps**	**27 Mbps**	**20-25 Mbps**
Frequency	5 GHz	2.4 GHz	2.4 GHz
Available Spectrum	300 MHz	83.5 MHz	83.5 MHz
Modulation Encoding	OFDM	DSSS/CCK	DSSS/PBCC
# Channels/ non-overlapping	12/8	11/3	11/3

IEEE 802.11 supports two types of access protocols in MAC layer: Distributed Access Protocol and Centralized Access Protocol. In Distributed Access Protocol, there is no central coordination, network is distributed in manner. It acts as an Ad Hoc Wireless Network. In Centralized Access Protocol, there is a central base station which connects a number of wireless stations.

VII. NETWORKING SECURITY

Networking security is the most important part in the Wireless LAN technology. To avoid the attacks and risks, a security protocol for Wireless LAN should satisfy the following properties:

- **Confidentiality-** The sender sends the data to the intended receiver and it is ensured that the message is comprehensible only by the intended receiver. It prevents the unauthorized usage and access to the network. For example, confidentiality ensures that an unauthorized user cannot derive any useful information about the person's passwords and security number. Data encryption ensures the confidentiality mechanism.
- **Integrity-** The security mechanism ensures that the message sent by the sender to the receiver or destination is unaltered. The unauthorized users cannot insert, delete, destroy and modify the data.
- **Availability-** Availability is the security protocol which ensures that the network must perform without any interruption. It should provide the guaranteed services and have the ability to tolerate the link failure as well as several attacks by the unauthorized individuals.
- **Non-repudiation-** This security mechanism ensures that the sender cannot deny of sending its message and the receiver cannot deny of receiving its message. Digital signature is the example of Non-repudiation.
- **Encryption and Authentication-** Encryption and authentication provide the ultimate security to the Wireless LAN technology. Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA) are the popular encryption methods in WLAN. Open Authentication, Shared Authentication and Expandable Authentication Protocol (EAP) are the popular authentication mechanisms.

VIII. GENERAL ATTACKS AND RISKS TO WLAN TECHNOLOGY

An attack is an action taken to destroy, expose and alter the information or data by unauthorized users in the network. Unlike the wired network, WLAN uses radio waves for communication; these actions have an intention to do harm. Attacks can be generally categorized in two types:

- Passive attack
- Active attack

Passive attack is the attempt made by the malicious nodes to obtain the information during transmission and reception without disrupting the network. Passive attacks are very difficult to detect as the operation of the network is not modified or altered by the attackers. Passive attacks can be classified as: Traffic analysis attack and Eavesdropping.

https://dx.doi.org/10.24001/ijaems.3.2.11 *ISSN: 2454-1311*

Active attacks are those types of attack in which attackers can alter the information or contents on the target and disrupt the operation of the network. Those active attacks are performed at the same network are known as internal attacks and those are performed outside the network are known as external attacks.

There are several attacks that can damage the WLAN. Some of them are as follows:

- Denial-of-Service
- Man in the Middle attack
- Spoofing and Session High jacking
- Eavesdropping
- Attack on Service Set Identifier
- Jamming

1. Denial-of-service

In this type of attack, the attacker floods the network with inconsistent data, packet, valid or in valid messages to put the burden on the resources and stop the utilization of the resources for the nodes which are present in the network. Thus the network is no longer operating as previously. This may lead to the failure of the delivery which was guaranteed to the end users. Due to the relatively low bit rates of WLAN, can leave them to open Denial-of-Service attacks. This illustrates the need for availability mechanism.

2. Man in the Middle attack

A Man in the Middle attack is the type of attack where the unauthorized user or attacker positions between the sender and the receiver in such a way that the attacker can read, intercept, modify and retransmit data to the intended receiver. Thus it breaks the integrity and confidentiality of data. This illustrates the need for integrity mechanism.

3. Spoofing and Session High jacking

In this form of attack, the attacker modifies the MAC address and acts as the valid access point. The attacker gets the license to access on the network and various resources such as printers, servers etc by assuming the identity of the valid user in the network as the 802.11 networks do not provide any authentication to the MAC address frame. Hence the MAC addresses are spoofed by the attacker and high jack the session.

4. Eavesdropping

This kind of attack refers to the reception of the message by an attacker. An unauthorized individual gain the access to the network, read the private data that is being transmitted across the network. Wireless LANs radiate network into space. This makes it impossible to control who can receive signals in any wireless LAN installation. Hence, the eavesdropping by third parties enables the attacker to intercept the transmission over the air from a distance [2]. Eavesdropping can be prevented by using confidentiality measures.

5. Attack on Service Set Identifier

Service Set Identifier refers to the identification of a network that provides the communication between the client and an appropriate access point. The access point was released in the market with the valid SSID and password. Hence, SSID provides a password authentication mechanism which makes the wireless local area network secured. There are two modes in SSID: open mode and closed mode. In open mode, SSID of access point is broadcasted and any network can connect in the public domain whereas in closed mode, the proper authentication is provided.

6. Jamming

Jamming attack can be introduced as international interference attacks due to the spontaneous emission of radio frequency signal in the MAC and the Physical layer of wireless networks. The attacker can interfere with legitimate traffic and could employ jamming signals which disrupts the ongoing transmission of the wireless channel. The main objective of the jamming is to block the reception of messages. Jamming attacks can be overcome by Frequency Hopping Spread Spectrum and Direct Sequence Spread Spectrum technique.

IX. CONCLUSION

In this paper, we have discussed about the Wireless LAN technology and its security system. In modern days WLAN is an important ongoing process as it becomes more popular, flexible and the ultimate solution of the communication system. Wireless LAN bears some advantages but every wireless protocol has some demerits. When this technology was introduced, hackers searched for security vulnerable, they exploit those vulnerabilities. Hackers cannot be eliminated. Hence, the organizations can mitigate these security problems of WLAN with proper planning, implementation, and management, constant maintenance and development of wireless standards.

REFERENCES

[1] “Ad Hoc Wireless Networks – Architectures and Protocols”- C. Siva Ram Murthy and B.S. Manoj
[2] R.A. Hamid, Wireless LAN: Security Issues and Solutions [Press release], 2003
[3] Stallings, Wireless Communication and Networks.
[4] http://www.cs.mun.ca/~yzchen/bib/80211_whitepaper.pdf
[5] http://www.sans.org/reading-room/whitepapers/wireless-lan-security-issues-solutions-1009
[6] WLAN Security Issues and Solutions by Deepika Dhiman

https://dx.doi.org/10.24001/ijaems.3.2.11 *ISSN: 2454-1311*

http://www.iosrjournals.org/iosr-jce/papers/Vol16-issue1/Version-4/J016146775.pdf

[7] Wireless LAN Security Threats and Vulnerabilities: a Literature review https://thesai.org/Downloads/Volume5No1/Paper_25-Wireless_LAN_Security_Threats_Vulnerabilities.pdf

[8] https://arxiv.org/ftp/arxiv/papers/1303/1303.1882.pdf