Evolution of Wireless LAN in Wireless Networks

Menal
Assistant Professor, Dept. of Computer Science
Maharaja Surajmal Institute
Janakpuri, Delhi, India
E-mail: menaldahiya@gmail.com

Abstract—**This paper discusses about the wireless networks, which enable multiple devices to connect without any physical connection. The evolution of a group of wireless network that is Wireless LAN which connects devices and network using an access point. The various factors of Wireless LAN are such as frequency and data rates, IEEE 802.11 architecture, components, range as well as its benefits. The security problems, enforce with the Wireless LAN as well as the risks and threats concerned with the security of Wireless LAN are explained.**

Keywords-IEEE 802.11; Wireless Networks; WLAN; WPAN; WMAN.

I. INTRODUCTION

Wireless Networks are becoming more and more popular now days in business as well as personal lives which is due to the advantages they offer. Advantages are such as: user mobility, fast and simple installation, flexibility, scalability, relatively low price etc.. Wireless technologies even offer Global Positioning System(GPS) that pinpoint the location of any device anywhere in the world and Personal Digital Assistants(PDA) which allow access to calendars, e- mail, phone number lists and internet. These advantages come from the medium that transfers the data – with the wireless networks, it is the air. Data are transferred via radio waves spreading throughout the space and thus the information reaches anyone with the appropriate radio receiver. Therefore, there is a problem of the protection of information. Traditional mechanisms for the physical protection of wired networks (firewalls and shields) cannot be applied to the protection of wireless networks. It was necessary to create mechanisms for the protection of the wireless networks in order to enable users to use wireless networks and feel sure about the accuracy of information and their privacy. Wireless networking is inherently insecure. There are a variety of attack methods that can be used against the users of wireless networks. Modern wireless data networks use a variety of cryptographic techniques such as encryption and authentication to provide barriers to such infiltrations. However, many of the commonly used security precautions are woefully inadequate. They seem to detract the casual sniffer, but are unable to stop the powerful adversary. New products and features are being introduced continuously. Many of these products now offer security features designed to resolve long-standing weaknesses or address newly discovered ones. Yet with each new capability, a new threat or vulnerability is likely to arise. Wireless technologies are evolving swiftly. Therefore, it is essential to remain abreast of the current and emerging trends in the technologies and in the security or insecurities of these technologies. Section I describes about Wireless Networks. Section II describes about Wireless LAN. Section III describes about the security of WLAN. Section IV describes about the security threats of WLAN. The purpose of this document is to find out some problems related to WLAN.

II. WIRELESS NETWORKS

Wireless Networks provide the transport mechanism among devices and the traditional wired networks. Wireless networks enable one or more devices to communicate without physical connections—without requiring network or peripheral cabling. Wireless Networks use radio frequency transmissions as the means for transmitting data, whereas wired technologies use cables. Wireless technologies range from complex systems, such as Wireless Local Area Networks (WLAN) and cell phones to simple devices such as wireless headphones, microphones, and other devices that do not process or store information. They also include infrared (IR) devices such as remote controls, some cordless computer keyboards and mice, and wireless hi-fi stereo headsets, all of which require a direct line of sight between the transmitter and the receiver to close the link. Wireless networks allow devices to be moved about with varying degrees of freedom and still maintain communication with each other. They also offer greater flexibility than cabled networks and significantly reduce the time and resources needed to set up new networks and allow for ad hoc networks to be easily created, modified or torn down. Wireless technologies use wavelengths ranging from the radio frequency (RF) band up to and above the IR band.2 The frequencies in the RF band cover a significant portion of the EM radiation spectrum, extending from

9 kilohertz (kHz), the lowest allocated wireless communications frequency, to thousands of gigahertz (GHz). As the frequency is increased beyond the RF spectrum, EM energy moves into the IR and then the visible spectrum [1,9].

Wireless networks are widely categorized into four groups based on their coverage range: Wireless Wide Area Networks (WWAN), Wireless Local Area Networks (WLAN), Wireless Metropolitan Area Networks (WMAN) and Wireless Personal Area Networks (WPAN).

A. Wireless Personal Area Network (WPAN)

It is a small-scale wireless network that requires little or no infrastructure and operates within a short range. A WPAN is typically used by a few devices in a single room instead of connecting the devices with cables. Examples include print services are enabling a wireless keyboard or mouse to communicate with a computer. WPAN, represents wireless personal area network technologies such as Bluetooth and IR. All of these technologies are "tether less"—they receive and transmit information using electromagnetic (EM) waves.

B. Wireless Local Area Networks (WLAN)

They are groups of wireless networking nodes within a limited geographic area, such as an office building or campus, that are capable of radio communications. WLANs are usually implemented as extensions to existing wired local area networks to provide enhanced user mobility. WLAN, representing wireless local area networks, includes 802.11, Hiper LAN, and several others.

C. Wireless Metropolitan Area Networks (WMAN)

It can provide connectivity to users located in multiple facilities generally within a few miles of each other. Many WMAN implementations provide wireless broadband access to customers in metropolitan areas.

D. Wireless Wide Area Networks (WWANS)

It connects individuals and devices over large geographic areas. Wireless WANs are typically used for mobile voice and data communications, as well as satellite communications. WWAN includes wide coverage area technologies such as 2G cellular, Cellular Digital Packet Data (CDPD), Global System for Mobile Communications (GSM), and Mobitex [2,10].

III. WIRELESS STANDARDS

Wireless technologies conform to a variety of standards and offer varying levels of security features. The principal advantages of standards are to encourage mass production and to allow products from multiple vendors to interoperate. The standards which are normally used are Wi-Fi technology, HiperLAN1/2, HomeRF and Bluetooth. 802.11, *802.11a, 802.11b/g/n,* and/or *802.11ac* wireless standards collectively known as Wi-Fi technologies. The IEEE designed 802.11 to support medium-range, higher data rate applications, such as Ethernet networks, and to address mobile and portable stations. European Telecommunications Standards Institute, ETSI, introduced High Performance Radio LAN (HiperLAN 1) standard in 1996 to provide high speed communications (20Mbps) between portable devices in the 5GHz range.

HiperLAN/1 supports isochronous traffic for different type of data such as video, voice, text, etc. Later, ETSI, rolled out in June 2000, a flexible Radio LAN standard called HiperLAN 2, designed to provide high speed access (up to 54 Mbps at PHY layer) to a variety of networks including 3G mobile core networks, ATM networks and IP based networks, and also for private use as a wireless LAN system. Basic applications include data, voice and video, with specific Quality of Service parameters taken into account. HIPERLAN/2 has a very high transmission rate up to 54 Mbps. Ad hoc networks follow proprietary techniques or are based on the Bluetooth standard, which was developed by a consortium of commercial companies making up the Bluetooth Special Interest Group (SIG). Bluetooth is an industry specification for short-range RF-based connectivity for portable personal devices with its functional specification released out in 1999. Bluetooth communicates on a frequency of 2.45 gigahertz, which has been set aside by international agreement for the use of industrial, scientific and medical devices (ISM). HomeRF is an open industry specification developed by Home Radio Frequency Working Group [2] that defines how electronic devices such as PCs, cordless phones and other peripherals share and communicate voice, data and streaming media in and around the home. HomeRF-compliant products operate in the license-free 2.4 GHz frequency band and utilize frequency-hopping spread spectrum RF technology for secure and robust wireless communications with data rates of up to 1 Mbps (HomeRF1). Unlike Wi-Fi, HomeRF already has quality-of-service support for streaming media and is the only wireless LAN to integrate voice. HomeRF may become the worldwide standard for cordless phones.

WLANs are based on the IEEE 802.11 standard, which the IEEE first developed in 1997. The IEEE designed 802.11 to support medium-range, higher data rate applications, such as Ethernet networks, and to address mobile and portable stations. 802.11 is the original WLAN standard, designed for 1 Mbps to 2 Mbps wireless transmissions. It was followed in 1999 by 802.11a, which established a high-speed WLAN standard for

the 5 GHz band and supported 54 Mbps. Also, completed in 1999 was the 802.11b standard, which operates in the 2.4 - 2.48 GHz band and supports 11 Mbps. The other Standards developed by IEEE are: 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac [3].

IV. WIRELESS LAN OVERVIEW

WLAN technology is experiencing tremendous growth which is due to increment in bandwidth made possible by the IEE 802.11 standard.

Early WLAN technologies had several problems like they were expensive, provided low data rates, were prone to radio interference, and were designed mostly to proprietary RF technologies. The 802.11 project is initiated in 1990 by IEEE to develop a Medium Access Control (MAC) and Physical Layer (PHY) specification for wireless connectivity for fixed, portable, and moving stations within an area." In 1997, IEEE first approved the 802.11 international interoperability standards. Then, in 1999, the IEEE ratified the 802.11a and the 802.11b wireless networking communication standards whose goal were to create a standards-based technology that could span multiple physical encoding types, frequencies, and applications. The 802.11a standard uses orthogonal frequency division multiplexing (OFDM) to reduce interference. This technology uses the 5 GHz frequency spectrum and can process data at up to 54 Mbps. Motorola developed one of the first WLAN technology [5].

A. Frequency and Data Rates

IEEE developed the 802.11 standards to provide wireless networking technology like the wired Ethernet that has been available for many years. The IEEE 802.11a standard operates in the licensed 5 GHz band using OFDM technology. The popular 802.11b standard operates in the unlicensed 2.4 GHz–2.5 GHz Industrial, Scientific, and Medical (ISM) frequency band using a direct sequence spread-spectrum technology. The ISM band has become popular for wireless communications because it is available worldwide. The 802.11b WLAN technology permits transmission speeds of up to 11 Megabits per second. The speed makes it considerably faster than the original IEEE 802.11 standard (that sends data at up to 2 Mbps) and slightly faster than standard Ethernet [6].

B. Wireless LAN Components

A WLAN comprises two types of equipment: a wireless station and an access point. A station, or client, is typically a laptop or notebook personal computer (PC) with a wireless NIC A WLAN client may also be a desktop or handheld device (e.g., PDA, or custom device such as a barcode scanner) or equipment within a kiosk on a manufacturing floor or other publicly accessed area. Wireless laptops and notebooks— "wireless enabled"—are identical to laptops and notebooks except that they use wireless NICs to connect to access points in the network. The wireless NIC is commonly inserted in the client's Personal Computer Memory Card International Association (PCMCIA) slot or Universal Serial Bus (USB) port. The NICs use radio signals to establish connections to the WLAN. The AP, which acts as a bridge between the wireless and wired networks, typically comprises a radio, a wired network interface such as 802.3, and bridging software. The AP functions as a base station in the wireless network, aggregating multiple wireless stations onto the wired network [7].

C. Range

The reliable coverage ranges for 802.11 WLANs depends on several factors, including data rate required and capacity, sources of RF interference, physical area and characteristics, power, connectivity, and antenna usage. Theoretical ranges are from 29 meters (for 11 Mbps) in a closed office area to 485 meters (for 1 Mbps) in an open area. However, through empirical analysis, the typical range of connectivity of 802.11 equipment is approximately 50 meters (about 163 ft.) indoors. A range of 400 meters, nearly ¼ mile, makes WLAN the ideal technology for many campus applications. It is important to recognize that special high-gain antennas can increase the range of several miles. APs may also provide a "bridging" function. Bridging connects two or more networks together and allows them to communicate—to exchange network traffic. Bridging involves either a point-to-point or a multipoint configuration. In a point-to-point architecture, two LANs are connected to each other via the 12 Notebook computers are basically the same as laptop computers, except that they are generally lighter in weight and smaller in size.

LANs' respective APs. In multipoint bridging, one subnet on a LAN is connected to several other subnets on another LAN via each subnet AP. Enterprises may use bridging to connect LANs between different buildings on corporate campuses. Bridging AP devices are typically placed on top of buildings to achieve greater antenna reception. The typical distance over which one AP can be connected wirelessly to another by means of bridging is approximately 2 miles. This distance may vary depending on several factors including the specific receiver or transceiver being used [11].

TABLE I. CHARACTERISTICS OF 802.11 WIRELESS LANS

Characteristic	**Description**
Physical Layer	Direct Sequence Spread Spectrum (DSSS), Frequency Hopping Spread Spectrum (FHSS), Orthogonal Frequency Division Multiplexing (OFDM), infrared (IR).
Frequency Band	2.4 GHz (ISM band) and 5 GHz.
Data Rates	1 Mbps, 2 Mbps, 5.5 Mbps (11b), 11 Mbps (11b), 54 Mbps (11a)
Data and Network Security	RC4-based stream encryption algorithm for confidentiality, authentication and integrity. Limited key management.
Operating Range	Up to 150 feet indoors and 1500 feet outdoors.
Positive Aspects	Ethernet speeds without wires; many different products from many different companies. Wireless client cards and access point costs are decreasing.
Negative Aspects	Poor security in native mode; throughput decrease with distance and load.

V. SECURITY OF WIRELESS LANS

The IEEE 802.11 specification identified several services to provide a secure operating environment. The security services are provided largely by the Wired Equivalent Privacy (WEP) protocol to protect link-level data during wireless transmission between clients and access points. WEP does not provide end-to-end security, but only for the wireless portion of the connection.

A. Security Features of 802.11 Wireless LANs

The three basic security services defined by IEEE for the WLAN environment are as follows:

- *Authentication*—WEP provides a security service to verify the identity of communicating client stations. In this the access control is provided to the network by denying access to client stations that cannot authenticate properly.
- *Confidentiality*—Confidentiality was developed to provide "privacy achieved by a wired network." The intent was to prevent information from casual eavesdropping.
- *Integrity*—This service ensures that messages are not modified in transit between the wireless clients and the access point in an active attack.

B. Authentication Secvices

- *Open System Authentication:* Open System authentication gives a NULL authentication in which it authenticates anyone who request for authentication. After the association of mobile, its data frames would be encrypted, if WEP was required in the WLAN. If WEP was not being used, the data frames will be sent in the clear, that means if there is no initial authentication, still data are encrypted.
- *Shared Key Authentication:* Shared key authentication uses a standard challenge and response along with a shared secret key to provide authentication. In this, the access point sends a string of unencrypted data to client and client encrypts with WEP key and sends back. This way of authentication is also insecure as a user sniffing the traffic would see the unencrypted and encrypted traffic.

VI. SECURITY THREATS OF WLAN

There has been tremendous growth and success of Wireless LAN, but there are also risks to security of Wireless LAN—i.e., attacks on confidentiality, integrity, and network availability.
Network security attacks are typically divided into passive and active attacks. These two broad classes are then subdivided into other types of attacks. All of them are defined below:

- *Passive Attack*—An attack in which an unauthorized party gains access to an asset and does not modify its content (i.e., eavesdropping). Passive attacks can be either eavesdropping or traffic analysis (sometimes called traffic flow analysis). These two passive attacks are described below:
- *Eavesdropping*—The attacker monitors transmissions for message content. The example of this attack is a person listening into the transmissions on a LAN between two workstations or tuning into transmissions between a wireless handset and a base station.
- *Traffic analysis*—The attacker, in a subtler way, gain intelligence by monitoring the transmissions for patterns of communication. A considerable amount of information is contained in the flow of messages between communicating parties.

- *Active Attack*—An attack in which an unauthorized party makes modifications to a message, data stream, or a file. It is possible to detect this type of attack, but it may not be preventable. Active attacks may take the form of one or a combination of four types: masquerading, replay, message modification, and denial-of-service (DoS). These attacks are defined below:
- *Masquerading*—The attacker impersonates an authorized user and thereby gains certain unauthorized privileges.
- *Replay*—The attacker monitors transmissions (passive attack) and retransmits messages as the legal user.
- *Message modification*—The attacker alters a legal message by deleting, adding to, changing, or reordering it.
- *Denial-of-service*—The attacker prevents or prohibits the normal use or management of communications facilities.

The consequences of these attacks include, but are not limited to, loss of proprietary information, legal and recovery costs, tarnished image, and loss of network service [12,15].

VII. CONCLUSION

This paper concludes that WLAN is mostly usable wireless network for a longer range and includes Wi-Fi which can connect multiple devices and can share data with security without any requirement of cables for connection. The main standard of WLAN is IEEE 802.11 which offers security using WEP protocol. There are multiple goals of security and attacks which are overcome by WLAN and enforces security to the critical data. Paper conclude some basic problems with WLAN. Problems with the IEEE 802.11 Standard Security are: - Security features in vendor products are frequently not enabled, Generation Algorithms are short (or static), Cryptographic keys are short, Cryptographic keys are shared, Cryptographic keys cannot be updated automatically and frequently, RC4 has a weak key schedule and is inappropriately used in WEP, Packet integrity is poor, no user authentication occurs, Authentication is not enabled; only simple SSID identification occurs, Device authentication is simple shared-key challenge-response, The client does not authenticate the AP.

REFERENCES

[1] http://en.wikipedia.org/wiki/Wireless_network.
[2] S. Gopala Krishnan, "A Survey Of Wireless Network Security," IJCSMC, Volume.03, Issue.01, pp.53–68, January 2014.
[3] IEEE 802.11-1999, "IEEE Standard for Local and Metropolitan Area Networks Specific Requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," June 12, 1999, **DOI:** 10.1109/IEEESTD.2003.95617.
[4] Ahmed M. Al-Naamany, Ali Ai Shidhani and H. Bourdoucen, "IEEE 802.11 Wireless LAN Security Overview," International Journal of Computer Science and Network Security, Volume06, Issue.5b, pp. 138-156, May 2006.
[5] Chapter 1 Introduction 1.1 Wireless Technology, http://shodhganga.inflibnet.ac.in/bitstream/10603/34313/10/09_chapter-1.pdf.
[6] Tom Karygiannis and Les Owens, "Wireless Network Security: 802.11,Bluetooth and Handheld Devices," Special Publication 800-48 NSIT, November 2002, https://www.yumpu.com/en/document/view/41640325/wireless-network-security-international-institute-of-information-/25.
[7] V Karamchand Gandhi, "A Study on Wireless LAN Fundamentals, Architecture, Benefits and Its Security Risks," Indian Streams Research Journal, Volume.04, Issue.08, September 2014, ISSN No : 2230-7850.
[8] Shivappa M Metagar, Dattatraya T Huvinahalli, Theja N and B. P. Savukar, "General Approach For Bluetooth Network Security System," International Journal of Research in Computer Applications and Robotics, Volume.01, Issue.03, June 2013.
[9] "Wireless Networking Choices for the Broadband Internet Home," HomeRF Working Group, 2001, http://www.cazitech.com/HomeRF%20WP%20-%20Wireless%20Choices.PDF.
[10] Aniruddha Singh, Abhishek Vaish and Pankaj Kumar Keserwani, "Research Issues and Challenges of Wireless Networks," International Journal of Advanced Research in Computer Science and Software Engineering, Volume.04, Issue.02,pp. 572-575, February 2014.
[11] Craig J. Mathias, "Wireless Security: Critical Issues and Solutions," COMNET, January 2003, http://www.webtorials.com/main/comnet/cn2003/wireless/43.pdf.
[12] Radomir Prodanovi and Dejan Simi, "A Survey of Wireless Security," Journal of Computing and Information Technology, Volume.15, Issue.03, pp. 237-255, 2007.
[13] "Wireless Networking Security" December 2010, http://www.infosec.gov.hk/english/technical/files/wireless.pdf.
[14] Vijay Chandramouli, "A Detailed Study on Wireless Technologies," 2002, https://www.uta.edu/oit/policy/ns/docs/wireless-paper-vijay.pdf.
[15] Yulong Zou, Jia Zhu, Xianbin Wang and Lajos Hanzo, "A Survey on Wireless Security: Technical Challenges, Recent Advances and Future Trends," IEEE Proc. On Information Theory, Cryptograpy and Security, May 2015.

AUTHORS PROFILE

Ms Menal is Assistant Professor of Computer Science at Maharaja Surajmal Institute(Affiliated to GGSIP University,Delhi) and a Research Scholar of Maharshi Dayanand University,Rohtak in the Dept. Of Computer Science and Applications. She received her MPhil in Computer Science from Chaudhary Devi Lal University, Sirsa, India in 2007.Before she had studied at Guru Jambheshwar University of Science & Technology (GJU), Hisar and KUK, Kurukshetra,India. Her main research interest are Neural Network,Wireless Security and Wireless Communication. Several of her research papers have been published in international peer-reviewed journals indexed in Scopus, ESCI, ICI and others.