"WIRELESS TECHNOLOGY IN NETWORK AND SECURITY ISSUES WITH WIRELESS FIDELITY (WI-FI)"

Teg Singh*
*Assistant Professor, Department of Computer Science, Govt. College Bilaspur (H.P.)

(Lt) Jagvinder Singh**
** Assistant Professor, Department Of Computer Application, GJIMT, Mohali.

ABSTRACT

Wireless technology provides us much profit like portability and flexibility, increased productivity and lower installation costs. Security issues have also been crossed a level in Wi-Fi network because of the unauthorized users and the Wi-Fi hackers. This research paper presents an overview regarding the emerging technology of wireless broadband networks. It focuses on the tools, standards and implementation of Wi-Fi networks. The purpose of this research paper is to understand the various problems associated with the implementation of these WLANs and purpose recommendation and measures to solve these problems.

KEYWORDS
Wireless Fidelity Technology, Qos, WLANs and Wi-Fi.

1. INTRODUCTION

Nowadays WLANs is more and more famous due to their reduced price of components, easy to deploy at anytime and anywhere in the world. End client are in a position to send big files through the communication medium that is air and free to move in the boundary of WLAN, able to access the internet and large bandwidth activities without the need of any cable or connectivity with a switch or a hub. Besides all of these advantage WLANs are facing the problem of security because many companies are transferring their sensible data across the WLANs so lots of people are doing research on the WLAN security. Wi-Fi allows user to surf internet at broadband speed when connected to access point (AP) or in ad hoc mode. The IEEE 802.11 architecture consists of several components that interact to provide a wireless LAN that support station mobility transparency to upper layers. The basic cell of an IEEE 802.11 LAN is called a basic service set (BSS), which is a set of mobile or fixed stations.

Wireless fidelity Wi-Fi technology is one of the upcoming techniques in the internet world. This Wi-Fi can be an alternate to wired technology. Wi-Fi is usually used for linking devices in wireless form. Wi-Fi Network attaches computers to one another in a better communicable way. It creates a hidden path between the internet and the wired network. Wi-Fi network functioning

can be done on the physical and the data link layer. Radio Frequency (RF) is used for transmitting data through air. This is the very characteristic in the Wi-Fi technology. It also provides enhanced data speeds. IEEE 802.11 is considered as a position of values moving elsewhere can be known as Wireless Local Area Network (WLAN). This is also a type of network communication.

Wi-Fi is a technology for WLAN based on the IEEE 802.11 (a, b, g) specifications. Originally developed for PC in WLAN Increasingly used for more services: Internet and VoIP phone access, gaming, and basic connectivity of consumer electronics such as televisions and DVD players, or digital cameras. In the future Wi-Fi will be used by cars in highways in support of an Intelligent Transportation System to increase safety, gather statistics, and enable mobile commerce (IEEE 802.11p). Wi-Fi supports structured (access point) and ad-hoc networks (a PC and a digital camera). An access point (AP) broadcasts its SSID (Service Set Identifier, "Network name") via packets (beacons) broadcasted every 100 ms at 1 Mbit/s. Based on the settings (e.g. the SSID), the client may decide whether to connect to an AP. Wi-Fi transmission, as a non-circuit-switched wired Ethernet network, can generate collisions. Wi-Fi uses CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) to avoid collisions. CSMA the sender before transmitting it senses the carrier if there is another device communicating then it waits a random time a retry. CA the sender before transmitting contacts the receiver and asks for an acknowledgement – if not received the request is repeated after a random time interval.

2. WIRELESS NETWORKS CHALLENGES

Wireless Networks plays the most important role in the development of the information in between individual-to-individual, business-to-business, and individual-to-business. It changed completely the way of sharing of the information but still there are lot of challenges which are the hurdles in the wide adaptation of wireless network technology [1], [2].we have to understand the main problems that not only WI-FI network faces but all the networks faces are –CIA that is confidentiality, integrity and authentication.

i) **Confidentiality:** Allow only the authorized person to read the encrypted messages or the information.

ii) **Integrity:** It is defined as the information not being opened by third person and it should reach in the same format as it was sent by the sending party.

iii) **Authentication:** The parties sending or receiving messages make sure that, who they say they are, and have right to undertake such actions. The main issue in the security of wireless signal is its mode of transmission. Wireless signals are transmitted through the electromagnetic waves; these waves cannot be contained physically. In wireless networks the signals are communicated via air, hence can be easily intercepted with the help of right transceiver equipment.

3. IEEE 802.11 STANDARDS

In 1997, IEEE ratified the 802.11 standard for WLANs. The IEEE 802.11 standard chains three transmission methods, including radio transmission surrounded by the 2.4 GHz band. In 1999, IEEE ratified two amendments to the 802.11 standard—802.11a and 802.11b—that describe radio transmission methods, and WLAN equipment based on IEEE 802.11b quickly became the leading wireless technology [10]. IEEE 802.11b equipment transmits in the 2.4 GHz band, contribution data rates of up to 11 Mbps. IEEE 802.11b was intended to provide performance, throughput, and security features comparable to wired LANs. In 2003, IEEE free the 802.11g amendment, which specifies a radio transmission method that uses the 2.4 GHz band and can carry data rates of up to 54 Mbps. Additionally, IEEE 802.11g-compliant products are backward compatible with IEEE 802.11b-compliant products [5],[6],[7].

3.1 WEP:

WEP protocol is element of the IEEE 802.11 standard [8], [9], [10], [11]. It was introduced in 1997.WEP is used in 802.11 network to defend link level data during the wireless transmission. WEP was the first cryptographic protocol which are developed for the WI-FI to facilitate privacy and authentication. WEP uses the shared key authentication mechanism and is based on secret cryptographic key. WEP protocol uses the RC4 (Rivest Cipher4) stream cipher algorithm to encrypt the wireless communications. This RC4 stream algorithm protects the contents form disclosure to eavesdroppers. WEP support 40-bit key and with addition it also support 128 or even 256 bit key also. WEP was designed to protect a wireless network from eaves dropping. WEP uses linear hash function for data integrity. In WEP there is no key management and no replay detection facility. But in 2001 several serious weaknesses were identified. Now, WEP connection can be cracked within minutes. After having such type of vulnerabilities, in 2003 the WI-FI Alliance WEP had been replaced by WPA. The main trouble of WEP was-it uses static encryption keys.

3.2 WPA/WPA2:

WPA and WPA2 are two security protocols developed by WI-FI Alliance .WPA provides developed with the point of solving the problems in WEP cryptographic method. WPA was developed in 2003. Both WPA and WPA2 have two modes of operation: Personal and Enterprise. The Personal mode involves the use of a pre-shared key for authentication, while the Enterprise mode uses IEEE 802.1X and EAP for this point.WPA2 was introduced in September 2004. WPA addresses a subset of the IEEE 802.11i specification that addresses the weaknesses of WEP. WPA2 extends WPA to include the full set of IEEE 802.11i requirements. WPA is easier to configure and it is extra secure than WEP. WPA uses the improved encryption algorithm known as TKIP (Temporal Key Integrated Protocol).TKIP provides each client with a unique key and uses much longer keys that are rotated at a configurable interval. It also includes an encrypted message integrity check field in the packets; this is designed to avoid an attacker from capturing, altering and/or resending data packets which prevent Denial-of-Service and spoofing attack. WPA can be operated with the help of RADIUS server of without RADIUS severs. Now, TKIP can be broken easily. WPA2 uses Advanced Encryption Standard. WPA2 may not work with some older network cards. WPA2 have the 4 main key factors:-

1. Mutual Authentication
2. Strong Encryption
3. Interoperability
4. Ease to Use

These are the 4 main advantages of WPA2. WPA and WPA2 use the cryptographic hash function for data integrity. WPA and WPA2 both provides the key management and replay detection.

4 WIRELESS LANS

Wireless LANs supply high performance within and around office buildings, factories, and homes. Table 1 provides some key characteristics at a glance.

Table 1: Key Characteristics of 802.11 Wireless LANs

Characteristics	Description
Physical Layer	Direct sequence spread spectrum (DSSS), Frequency hopping spread spectrum (FHSS), orthogonal frequency division multiplexing (OFDM), and 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 &Network Security	RC4-based stream encryption algorithm for Confidentiality, authentication, and integrity. Limited key management. (AES is being Considered for IEEE 802.11i.)
Operating Range	Up to 150 feet indoors and 1500 feet outdoors.9
Negative Aspects	Poor security in native mode; throughput Decrease with distance and load.

Wireless LANs consist mainly of two entities: clients or end-user devices and Access Points. The basic structure of a Wireless LAN is called infrastructure WLAN or BSS (Basic Service Set) shown in figure 1, in which the network consists of an access point and several wireless devices. When these devices try to communicate among themselves they propagate their data through the access point device.

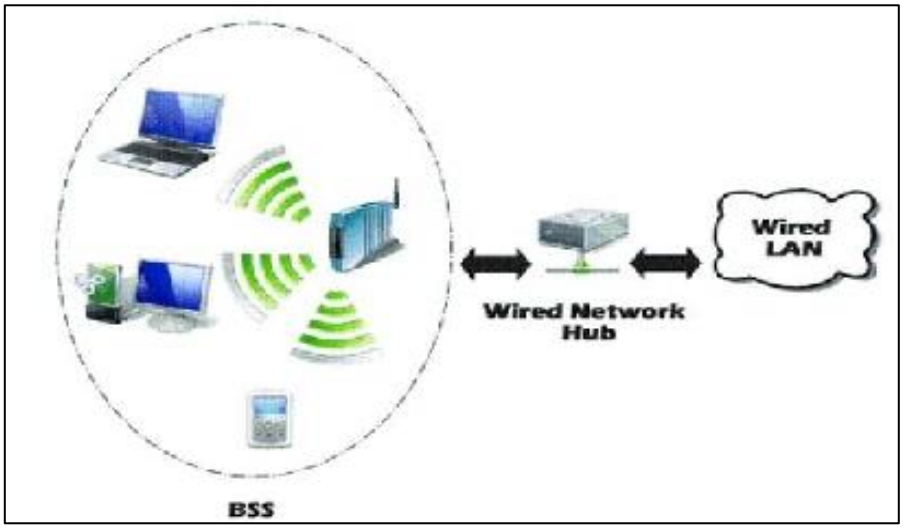

Figure 1: Wireless LANs (BBS structure)

If the BSS did not have an access point device, and the wireless devices were communicating with each other directly, this BSS is called an Independent BSS and works in mode called "ad hoc mode" (shown in figure2). Ad hoc networks are also commonly referred to as peer-to-peer networks [12], [13].

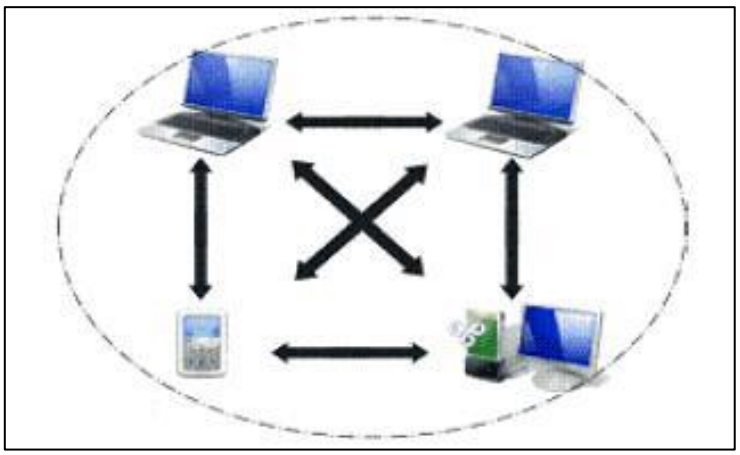

Figure 2: Ad hoc Wireless LANs

5. EXISTING TECHNOLOGIES AND PROBLEMS

The basic existing technology for implementation of Wireless networks (WLAN) in residential and enterprise setups can be understood simply from these explanatory diagrams.

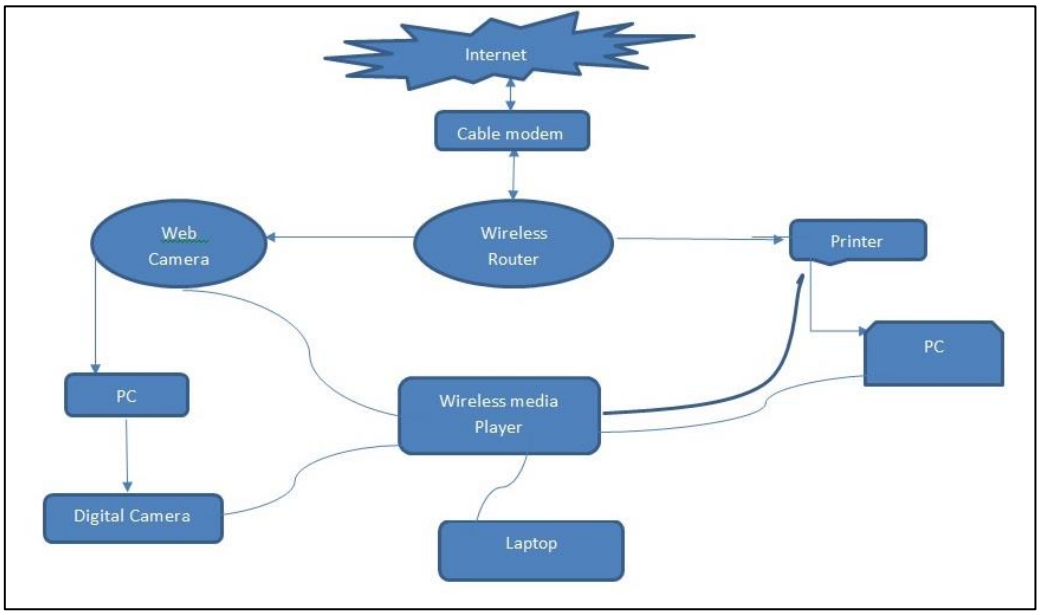

Figure 3: Wireless Router Network Diagram

However our major concern in this research paper is that there are several issues associated with the deployment and management of WLAN. These include scalability, provisioning, real-time and non-real time data flow, accessibility range, power management interference from other systems operating in the same spectrum such as Bluetooth.

Major problems that we need to address are:-

1. Security Management

2. QoS (Quality of Service) and centralized Management of WLANs.

6. OBJECTIVES OF STUDY

Following are the major objectives of study:

1) To study the various Vulnerabilities and attacks on WLAN and their solutions.

2) To study the some of the exiting security methods used for securing WLAN and explore the possibility of improvements in the same.

3) To analyze the various techniques based on misuse detection or anomaly detection for securing WLAN.

4) To develop new efficient security measures.

5) To study number of commercial available security solutions.

7. SOLUTIONS BASED ON RESEARCH

Recommendations for Secure Wireless Networks

1. Maintain a full understanding of the topology of the wireless network.

2. Label and keep inventories of the fielded wireless and handheld devices.

3. Perform periodic security testing, audits and assessment of the wireless network

4. Create backups of data frequently.

5. The information system security policy should directly address the use of 802.11, Bluetooth, and other wireless technologies.

6. Security training is essential to raise awareness about the threats and vulnerabilities inherent in the use of wireless technologies.

7. Perform a risk assessment, develop a security policy, and determine security requirements before purchasing wireless technologies.

8. Apply security management practices and controls to maintain and operate secure wireless networks after careful installation.

9. Configuration/change control and management practices should ensure that all equipment has the latest software release, including security feature enhancements and patches for discovered vulnerabilities.

10. Standardized configurations should be employed to reflect the security policy, and to ensure change of default values and consistency of operations.

11. Security training is essential to raise awareness about the threats and vulnerabilities inherent in the use of wireless technologies.

12. Robust cryptography is essential to protect data transmitted over the radio channel, and theft of equipment is a major concern. [3], [4].

8. CONCLUSION

Wi-Fi security is not an easy task. Wireless network security is more difficult than wired network security. Even WLANs increase client's productivity, they expose the network to a new group of hackers because WLAN works on OTA. Initial findings indicate that wireless security is still a serious issue in society today irrespective of residential or commercial networks. In the research work it is observed that many organizations are currently deploying wireless networks typically to use IEEE 802.11b protocols, but technology used is not secure and still highly susceptible to active attacks and passive intrusions.

REFERENCES

[1] Wireless security: an overview by Robert J. Boncella. Washburn University ZZbonc@washburn.bdu.

[2] White paper: WLAN security Today: wireless more secure than wired by Siemens Enterprise Communications.

[3] 3GPP: Standards organization associated with ITU.

[4] Gast, Matthew (2005), 802.11 Wireless Networks: The Definitive Guide, 2nd Edition, And O'Reilly Media.

[5] International Journal of Scientific & Engineering Research, Volume 3, Issue 8, August-2012, ISSN 2229-5518.

[6] IEEE Std. 802.11 i/D30 (2002) ,Wireless Medium Access Control (MAC) and physical Layer (PHY) Specification for enhanced Security.

[7] Establishing wireless robust security networks: a guide to IEEE 802.11i by Sheila Frankel Bernard Eydt Les Owens Karen Scarf one.

[8] The state of WI-FI security by WI-FI Alliance.

[9] WI-FI security –WEP, WPA and WPA2 by Guillaume Lehembre.

[10] WEP, WPA, WPA2 and home security by Jared Howe.

[11] Dr. Andy Ju a Wang Spring (2004), "Wireless LAN Security Research Paper IT 6823 Information Security Instructor".

[12] International Journal of Computer Science Trends and Technology (IJCST) – Volume 4 Issue 2. Mar - Apr 2016.

[13] Borison.N (UC Berkeley), Goldbery. I (Zero- Knowledge Systems), and Wagered (UC Berkeley) (2001),"Intercepting Mobile Communications: The Security of 802.11,"