ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)
Volume 5, Issue 6, June 2016

WiFi Technology

Monika Kumthekar, Madhuri Patil
MCA(IMCOST), Mumbai University C-4,Wagle Industrial Estate,
Thane Check Naka(W),Mumbai-400 607

ABSTRACT

Technology is making rapid progress and is making many things easier.As the innovative thinking of persons is increasing day-by-day,new methods for wireless networking has been evolved of which our present topic Wi-Fi is the most accepted technology. Wi-Fi, an acronym for Wireless-Fidelity which is the wireless way to handle networking. The main aim of this paper is wireless networking achieved by Wi-Fi. This paper introduces Wi-Fi technology and state of this technology in brief. We then deal with the different ways of wireless networking, connecting wi-fi and with wi-fi security and IEEE 802.11 Standards. This paper concludes with the pros and cons of this technology and it's future.

Keywords

Wi-Fi, Cloud , IEEE standards, WEP, WLAN

1. INTRODUCTION

1.1Wi-Fi's Walkie-Talkie Network

Wi-Fi, an acronym for "Wireless Fidelity", is a set of product compatibility standards for Wireless Local Area Networks (WLAN) based on the IEEE 802.11 specifications. Wi-Fi was intended to be used for mobile devices and LANs, but is now often used for Internet access. It enables a person with a wireless-enabled computer or personal digital assistant (PDA) to connect to the Internet when in proximity of an access point.

Wireless Fidelity is the wireless way to handle networking. It is also known as 802.11 networking and wireless networking. Using this technology we can connect computers anywhere in a home or office without the need of any wires. The computers connect to the network using radio signals, and they can be up to 100 feet or so apart.

Wi-Fi allows to connect to the internet from virtually anywhere at speeds of up to 54Mbps.The computers and handsets enabled with this technology use radio technologies based on the IEEE 802.11 standard to send and receive data anywhere within the range of a base station.

Wi-Fi goes beyond wirelessly connecting computers, it also connects people.

2. WIRELESS NETWORK

2.1.Wi-Fi's Walkie-Talkie Network

Wi-Fi, an acronym for "Wireless Fidelity", is a set of product compatibility standards for Wireless Local Area Networks (WLAN) based on the IEEE 802.11 specifications. Wi-Fi was intended to be used for mobile devices and LANs, but is now often used for Internet access. It enables a person with a wireless-enabled computer or personal digital assistant (PDA) to connect to the Internet when in proximity of an access point.

Wireless Fidelity is the wireless way to handle networking. It is also known as 802.11 networking and wireless networking. Using this technology we can connect computers anywhere in a home or office without the need of any wires. The computers connect to the network using radio signals, and they can be up to 100 feet or so apart.

Wi-Fi allows to connect to the internet from virtually anywhere at speeds of up to 54Mbps.The computers and handsets enabled with this technology use radio technologies based on the IEEE 802.11 standard to send and receive data anywhere within the range of a base station.

Wi-Fi goes beyond wirelessly connecting computers, it also connects people.

2.2Wi-Fi's Radio Technology:

The radios used in Wi-Fi are not so different from the radios used in walkie-talkies. There are three big differences between Wi-Fi radios and Walkie-talkies.

WiFi radios that work with the 802.11b and 802.11g standards transmit at 2.4 GHz, while those that comply with the 802.11a standard transmit at 5 GHz. Normal walkie-talkies normally operate at 49 MHz. The higher frequency allows higher data rates.

WiFi radios use much more efficient coding techniques that also contribute to the much higher data rates. For 802.11a and 802.11g, the technique is known as orthogonal frequency-division multiplexing (OFDM). For 802.11b, it is called Complementary Code Keying (CCK).

The radios used for WiFi have the ability to change frequencies. 802.11b cards can transmit directly on any of three bands, or they can split the available radio bandwidth into dozens of channels and frequency hop rapidly between them. The advantage of frequency hopping is that it is much more immune to interference and can allow dozens of WiFi cards to talk simultaneously without interfering with each other.

3.Connecting Wi-Fi

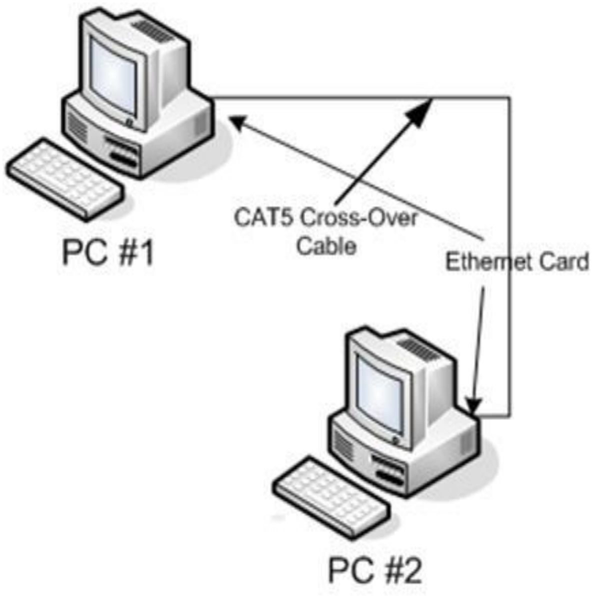
3.1.Adding WiFi to a Computer:

Many new laptops come with a Wi-Fi card built in. It is also easy to add a Wi-Fi card to an older laptop or a desktop PC. The process is

Take a 802.11a, 802.11b or 802.11g network card. 802.11g has the advantage of higher speeds and good interoperability on 802.11b equipment.

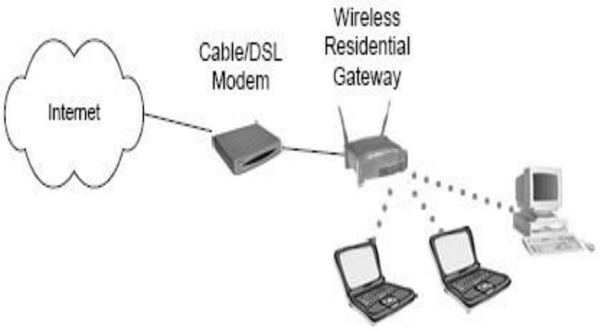
For a laptop, this card will normally be a PCMCIA card that slide into a PCMCIA slot on laptop. Or take a small external adapter and plug it into a USB port.

For a desktop machine, take a PCI card & install inside the machine, or a small external adapter and connect to the computer with a USB cable.



HOTSPOT:

It is a small box that is hardwired into the Internet. The box contains an 802.11 radio that can simultaneously talk to up to 100 or so 802.11 cards. There are many Wi-Fi hotspots now available in public places like restaurants, hotels, libraries and airports. We can create our own hotspot in our home.



3.2Configuring WiFi:

On the newest machines, an 802.11 card will automatically connect with an 802.11 hotspot and a network connection will be established. As soon as we turn on our machine, it will connect and we will be able to browse the web, send email, etc using Wi-Fi. On older machines we often have to go through this simple 3-step process to connect to a hotspot:

Access the software for the 802.11 card- normally there is an icon for the card down in the system tray at the bottom right of the screen.

Click the "Search button" in the software. The card will search for all of the available hotspots in the area and shows a list.

Double-click on one of the hotspots to connect to it.

On ancient 802.11 equipment, there is no automatic search feature. We have to find what is known as the SSID (server set id) of the hotspot (usually a short word of 10 characters or less) as well as the channel number (an integer between 1 and 11) and type these two pieces of information in manually. All the search feature is doing is grabbing these two pieces of information from the radio signals generated by the hotspot and displaying them for us.

4.Wi-Fi Security:

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.

Confidentiality: Allow only the authorised person to read the encrypted messages or the information.
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.
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 can not be contained physically. In wireless networks the signals are communicated via air, hence can be easily intercepted with the help of right transceiver equipment.

5.Hotspot in Home:

5.1.Setting up a Hotspot in a Home:

It is very easy to set up a Wi-Fi hotspot in home. It can be done in one of the two ways:
If there are several computers hooked together on an Ethernet network and want to add a wireless hotspot to the mix, purchase a Wireless Access Point and plug it into the Ethernet network.
If it is the first time to set up a network in home, or to upgrading, buy a Wireless Access Point Router. This is a single box that contains: 1) a port to connect to cable modem or DSL modem, 2) a router, 3) an Ethernet hub, 4) a firewall and 5) a wireless access point. Connect the computers to this box either with traditional Ethernet cables or with wireless cards.
Either way, once turn our Wireless Access Point on, there is a Wi-Fi hotspot in house. In a typical home, the new hotspot will provide coverage for about 100 feet (30.5 meters) in all directions, although walls and floors do cut down on the range. Even so, we get good coverage throughout a typical home. For a large home, buy inexpensive signal boosters to increase the range of the Hotspot.

5.2.Configuring a New Hotspot in Home:

Searching for hotspot

Most wireless access points come with default values built-in. Once we plug them in, they start working with these default values in 90 percent of the cases. However, we may want to change things. You normally get to set three things on the access point:
The SSID -- it will normally default to the manufacturer's name. We can set it to any word or phrase.
The channel -- normally it will default to channel 6. However, if a nearby neighbor is also using an access point and it is set to channel 6, there can be interference. Choose any other channel between 1 and 11. An easy way to see if our neighbors have access points is to use the search feature that comes with your wireless card.
The WEP key -- The default is to disable WEP. To turn it on, enter a WEP key and turn on 128-bit encryption.
Access points come with simple instructions for changing these three values. Normally do it with a Web browser. Once it is configured properly, we can use our new hotspot to access the Internet from anywhere in our home.

6.Advantages of Wi-Fi:

1. Wi-Fi is a core technology in GPS Industries Applications.
2. Wi-Fi technology available in hotels, airports, etc., will be more inclined to bring laptop with us when traveling for personal reasons.
3. Frees network devices from cables, allows for a more dynamic network to be grown.
Changes the way people live, communicate, work and play.
4. Give team-based workers the ability to access the network.
5.It helps to become more productive at home, like online shopping and banking;
6. Wi-Fi technology allows getting out of home office and working in other rooms.

6.Disadvantages of Wi-Fi:

1.The 802.11b and 802.11g flavors of Wi-Fi use the 2.4 GHz spectrum, which is crowded with other devices such as Bluetooth, microwave ovens, cordless phones, or video sender devices, among many others.
2.Power consumption is fairly high compared to other standards, making battery life and heat a concern.
3.It is not always configured properly by users.
4.Security techniques are not reliable yet.

7. IEEE 802.11 Standards

In 1997, IEEE ratified the 802.11 standard for WLANs. The IEEE 802.11 standard supports three transmission methods, including radio transmission within the 2.4 GHz band. In 1999, IEEE ratified two amendments to the 802.11 standard—802.11a and 802.11b—that define radio transmission methods, and WLAN equipment based on

IEEE 802.11b quickly became the dominant wireless technology [10]. IEEE 802.11b equipment transmits in the 2.4 GHz band, offering 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 released the 802.11g amendment, which specifies a radio transmission method that uses the 2.4 GHz band and can support data rates of up to 54 Mbps. Additionally, IEEE 802.11g-compliant products are backward compatible with IEEE 802.11b-compliant products.[7].

IEEE Standard or Amendment	**Maximum Data Rate**	**Typical Range**	**Frequency Band**	**Comments**
802.11	2 Mbps	50-100 meters	2.4 GHz	
802.11a	54 Mbps	50-100 meters	5 GHz	Not compatible with 802.11b
802.11b	11 Mbps	50-100 meters	2.4 GHz	Equipment based on802.11b has been the dominant WLAN technology
802.11g	54 Mbps	50-100 meters	2.4 GHz	Backward compatible with 802.11b

Summary of IEEE 802.11 WLAN Technologies

WEP:- WEP protocol is part of the IEEE 802.11 standard [3], [8], [9], [10], [11], [13]. It was introduced in 1997.WEP is used in 802.11 network to protect link level data during the wireless transmission. WEP was the first cryptographic protocol which are developed for the WI-FI to enable 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 extension 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 problem of WEP was-it uses static encryption keys..

WPA/WPA2:-

WPA and WPA2 are two security protocols developed by WI-FI Alliance [9], [10], [11], [13]. WPA provides developed with the purpose 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 purpose.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 more 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 prevent 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.

The fundamental aspect of Wireless Networks in maintaining security is to maintain Confidentiality where the receiver should receive the actual transmitted information from the sender. The message authentication provides integrity to both sender as well as receiver. The Wireless Link should be always available and should be secured from outside world like malicious attacks as well as DoS Attacks (Denial of Service Attacks). In the case study the researchers define database schema for orders, contracts, project information, and business scenarios. The data is stored in module 2 in the DB2 database. Then there are schema for users and groups. This is also stored in the DB2 database. A technology called Enterprise Services Bus (ESB) is used to handle all information routing and transformation in the cloud information architecture module. ESB is designed by IBM to interact with WebSphere and provides integration for SOA applications. It is a software architecture model for communication between interacting software.

There are basically two common attacks which compromise the security and authentication mechanism of Wireless Networks i.e. Message Reply Attack and Man in the Middle Attack. The Message reply attack acts principally on the authentication and authentication key formation protocols. The Man in the Middle Attack (MiTM) attack occurs on that security mechanism which doesn't provide mutual authentication.

Various other attacks like Session Hijacking, Reflection attacks are there which affects the security mechanism of Wireless Networks.

IEEE helped in securing the wireless networks by providing the basic measures for securing wireless network and it also provide CIA factors by disabling SSID, use of MAC i.e. Media Access Control address filtering and WPA/WPS protection mechanism. The recent developments in computer technology and software developments notice that these mechanisms have network vulnerable attack. So, due to these vulnerabilities WiMax standards comes into existence, for solving the short comings of 802.11 wireless networks [4]. WiMax is the new advancement in the wireless network. WiMax is still undergoing development and still the securing problems are not being decreased by WiMax technology. It also has some drawbacks like it lack mutual authentication and is suspected to relays attacks, spoofing of MAC address of Subscriber Station (SS) and PMK authorization vulnerabilities.

8.SPECIAL FEATURES OF Wi-Fi

Unlike today's wired network, a Wi-Fi network requires little more than an access point(AP). Access to a Wi-Fi- network does not require an expensive connection to each user. Wi-Fi technology is also far less expensive to deploy than the limited wireless technologies of currently existing cellular servicing providers.

Access to a Wi-Fi broad band can be provided both outdoors and indoors. Whether from an outdoor café or a park bench a person can access the Internet if they are in range of a service station. Such a Wi-Fi broadband is much power full and can transmit data at a rate of 11Mbps which is sufficient for all types of multimedia.

Many schools and businesses have unsuitable building layouts or walls that cannot be wired for various reasons making it difficult or impossible to build a wired network. Wi-Fi is a very cost effective alternative in these environments.

A Wi-Fi network can provide many benefits for the society. It can provide local hospitals.

Though the radio waves are of relatively high frequency, they are not powerful enough to pass through multiple layers of building materials. Specifically radio waves are completely blocked by steel. For this reasons the factors deciding performance are proximity to access point and the degree to which the signal is blocked by the surroundings.

As more computers begin to communicate with the same access point ,a bottleneck occurs. An access point has a finite amount of network bandwidth to which it is physically linked. As a result, all computers that are associated with a specific access point must share the same bandwidth. More computers means the possibility for a slower network connection.

Since Wi-Fi technology is constantly improving these shortcomings will get removed soon.

10. CONCLUSION

As Wi-Fi is now shipped in millions of products and deployed in millions of homes, business and hotspots worldwide, the technology has moved beyond the realm of a computer feature. Wi-Fi has fast become a cultural phenomenon.

Wi-Fi security is not an easy task. Wireless network security is more difficult than wired network security. There are many protocols or standards or we can say technologies for wireless network security but every protocol has its demerits, until now there is no protocol which can provide security 100% or near about it.

11. 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] Sara Nasre Wireless Lan Security Research Paper IT *6823* Information Security Instructor: Dr. Andy Ju An Wang Spring *2004*.

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

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

[7] IEEE. Wirless LAN Medium Access Control (MAC) and Physical Layer (PHY) Speci_cations, IEEE std 802.11-1997 edition, 1997.

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

[9] Wireless network security? Author:-Paul Asadoorian, GCIA, GCIH. Contributions by Larry Pesce, GCIA , GAWN PaulDotCom.