Wi-fi Networking - An Overview

Prof. R. S. Balasubramanian, G. Balaji

Abstract

Wireless Fidelity (Wi-Fi) is a set of product compatibility standards for wireless local area network (WLAN) based on the IEEE 802.11 specifications. Wi-Fi was intended to be used for mobile devices, LANs and internet access through Access Points. Wi-Fi allows users to roam around the campus with a Laptop equipped with a wireless LAN card/adapter and stay connected to their network wirelessly. The wireless LAN uses either IR rays or RF radio waves for data exchange. Wireless communication is one of the fastest growing technologies. Wireless LAN represents a spectrum of capabilities that support limited distance coverage, longer distance coverage based on the power of transceivers.

Keywords: Radio waves, Hotspots, Performance, Rate shifting, Wired Equivalent Privacy (WEP), Wi-Fi protected access (WPA).

WIRELESS LOCAL AREA NETWORK

Wireless LAN is a networking system in which data is sent and received via high frequency radio waves. The systems are connected to the network through Access points called Hotspots.

Wireless communication between the system and Access points occurs through RF transmission or IR transmission.[1]-[3]

RF technology has frequencies in 1 to 20 GHZ and can be used to transmit data between stations in a wireless LAN. RF signals are transmitted using narrow band technique or spread spectrum technique. Narrow band uses Microwave frequencies. Because of interference of different networks, narrow band has very limited applications in wireless LAN.

Spread spectrum technique requires a bandwidth that is several times the original bandwidth. This is achieved by two techniques

1.Frequency hopping:

In this the sender sends on one carrier frequency for a short period of time, then hops to another carrier frequency for the same period of time, hops again to another for the same period of time and so on.

2. Direct sequence spread spectrum:

In this technique each bit to be sent is replaced by a sequence of bits called a chip code. (1-000111, 0-110011)

InfraRed has wavelength between 800-900 nm. Infrared transmission techniques are

1. Point-point:

The LAN features point-point links between computers, bridges, or switches.

2. Diffused:

The diffused IR LAN uses à reflecting object, where the reflected signals are received by all stations on the network.

WLAN SERVICES (BSS & ESS):

The IEEE 802.11 standard for wireless LAN defines two kinds of service (i) Basic Service Set (BSS) and (ii) Extended Service Set. (ESS)

Department of Information Technology,
Karpagam College of Engineering, Coimbatore-32

Basic Service Set:

Basic Service Set is defined as the building block of a wireless LAN. A BSS is made up of stationary or mobile wireless station and a possible central base station, known as Access Point. (AP)

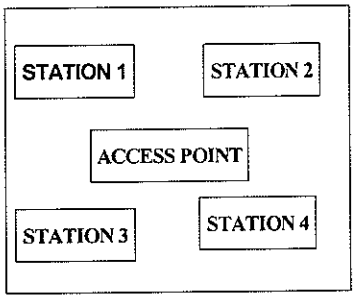

Fig 1: BSS with an AP

Extended Service Set:

An ESS is made up of two or more BSS with AP's. In this the BSS are connected through a distributed system which is usually wired. The distribution system connects the Access Points in BSS. ESS uses mobile and stationary stations. The mobile stations are normal stations inside a BSS. The stationary stations are AP stations that are the part of a wired LAN. Communication between tow stations occurs via Access Point.

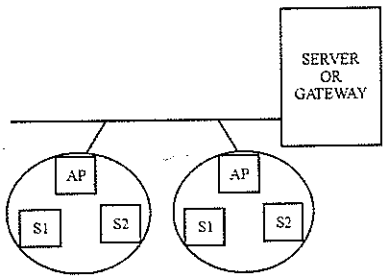

Fig2:ESS with two BSS AP-access point
S1-S2-mobile devices

WI-FI:

The wireless LAN adapter can be made to fit on a personal computer memory card industry association (PCMCIA) card for a laptop. Different specifications of IEEE 802.11 include 802.11b, 802.11a, 802.11g etc.

Wi-Fi is generically meant to refer any type of 802.11 network whether it is 802.11b, 802.11g etc. Wi-Fi is rapidly gaining acceptance in many companies as an alternative to a wired LAN.

Wi-Fi is specified in 802.11b specification from IEEE and is a part of series wireless specification together with 802.11, 802.11a, 802.11g. All the different wireless specifications use Ethernet protocol and CSMA/CA technology.

Instead of moving data through a network using Ethernet cable, Wi-Fi (802.11b) uses radio waves operating at 2.4 GHz offering a data rate of 11mbps.

MODULATION TECHNIQUE

Though there are different modulations for wireless LAN such as Binary phase shift keying (BPSK), Quadrature Phase Shift Keying (QPSK), and Complementary Code Keying (CCK) Wi-Fi employs CCK modulation.[4]-[5]. CCK modulation uses a complex set of functions known as complementary codes to send more data. CCK suffers less for multipath distortion i.e.) reduces RF interference that occur when radio signal has more than one path between the transmitter and receiver.

TRANSMISSION TECHNIQUE

802.11 standards employ FHSS and DSSS and Orthogonal Frequency Division Multiplexing (OFDM). The benefit of employing OFDM is high spectral efficiency, resilience to RF interference and lower multipath distortion.

OFDM works by breaking one high speed data carrier into several lower speed Subcarrriers, which are then transmitted in parallel. Each high speed carrier is 20 MHz wide and is broken into 52 channels, each approximately 300kHz wide. OFDM uses 48 channels for data and the remaining 4 channels for error correction. OFDM uses the spectrum much more efficiently by spacing the channels much closer together. The spectrum is more efficient

because all carriers are orthogonal to one another, thus preventing interference between closely spaced carriers.

WLAN REQUIREMENTS

The most common components for implementing WLAN environment are Laptops-Workstation, Adapters, Access Points, Bridges, and Antennas.

LAPTOPS

The most common device used on WLAN is workstation which includes laptop and desktop models. The difference between laptop and desktop is the Laptops has PCMCIA card. The greater advantage of Wi-Fi complaint device is that many laptops and PDA are now shipping with internal wireless NIC's installed. So ithout any modifications these devices can interoperate with each other. In other case the processor must be bundled with Peripheral component Interconnect (PCI) WLAN adapter to provide wireless connectivity.

MOBILE COMPUTING OPERATING SYSTEMS

Several Operating Systems are used on mobile computers. The primary ones include MSDOS, PALM OS, SYMBIAN OS, and WINDOWS CE AND WINDOWS XP. SYMBIAN OS is an open standard OS, licensed for use in many mobile computing devices and easily customized with third party. The mobile computer must be interoperable with desktop PC protocol, if not additional software might be needed for interoperability, speed, reliability, and real time communications.

CLIENT AND ADAPTERS

The wireless LAN adapters or NICs are radio modules that provide transparent data communication between fixed, portable or mobile wireless devices. The primary function of the client adapters is to transfer data packets transparently through the wireless infrastructure. The NIC's operate at layers 1 and 2 of the OSI model.

ACCESS POINTS

Access Point acts as a central communication point for wireless network users. An access point can link wire and wireless networks. In large installations, the roaming functionality provided by multiple AP's allows wireless users to move freely without any interruptions. Access point's important features are

1. Integrated Network Management:

Supports for SNMP and syslog to interface with existing network management is essential.

2. System security: It should be possible to restrict access to the AP management system to a list of users. Encryption should be supported, as well as Wired Equivalent Privacy (WEP) or dynamic WEP.

3. Filtering:

Protocol Filters are required to prevent or allow the use of the specific protocols through the AP. Controls for unicast and multicast packet forwarding and filtering, should also be present.

4. Firmware:

Firmware should be upgradeable and should support copying and restoring a configuration.

5. Standby assignment:

This feature allows AP to act as a backup for another AP to provide uninterrupted network connectivity.

6. World mode for international travelers:

Frequency regulation varies slightly over the world. This function allows a visitor from Japan using world mode on a client device to associate to an AP in the U.S and automatically switch to the correct regional settings.

7. Load balancing:

This feature automatically directs client's devices to an AP that provides the best connection to the network

based on the factors such as the number of users, bit-error rates, and available radio band width and signal strength.

BRIDGES

Bridges are designed to connect two or more networks that are typically located in different buildings. It delivers high data rates and superior throughput for data intensive line of sight applications. Bridges can be configured for point - point and point – multipoint applications.

ANTENNAS

Antennas have three fundamental properties Gain, Direction, and Polarization. Gain is the measure of increase in power. Direction is the shape of transmission patterns. Polarization is physical orientation of elements on the antenna that actually emits RF energy.

ASSOCIATION PROCESS OF CLIENTS AND ACCESS POINTS

Steps involved in association are

1. Client sends Probe request to the AP.
2. AP sends Probe response to the client.
3. Client evaluates AP response, and selects the best AP
4. Client sends authenticated request to selected AP(A)
5. AP(A) confirms authentication and registers client.
6. Client sends association request to selected AP(A)
7. AP(A) confirms association and registers client.

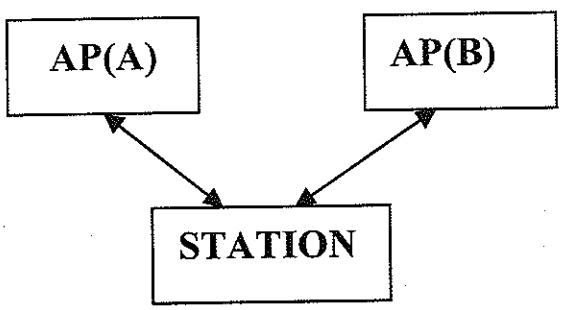

Fig 3: Association and Reassociation of client with AP

REASSOCIATION PROCESS OF CLIENTS AND ACCESS POINTS ON ROAMING

The steps involved in reassociation are,

1. Adapter listens for a beacon frame from AP's.
2. Adapter evaluates AP beacon and selects the best AP.
3. Adapter sends association request to selected AP (B).
4. AP(B) confirms association and registers adapter
5. AP(B) informs the reassociation with AP(A).

WI-FI PERFORMANCE PARAMETERS

Performance is used to describe the maximum data rate of the device, the actual throughput that the device provides, and the range of the radio waves in the device.[6]

DATA RATES SUPPORTED BY WI-FI

The Wi-Fi LAN equipment is most commonly promoted as providing a maximum data rates of 11 mbps. The IEEE 802.11b specification, that rests as foundation for Wi-Fi actually support a total of four data rates 1,2,5.5,11 Mbps.

The data rates are available on the same physical medium. Specifically, 80 MHz wide portion of radio frequency spectrum, starting at 2.4 GHz that is divided into between 11 to 14 channels.

The base for four data rates provided by 802.11b standard is three different modulation types,

1. Binary Phase Shift Keying (BPSK) for 1Mbps
2. Quadrature Phase Shift Keying (QPSK) for 2 Mbps
3. Complementary Code Keying (CCK) for 5.5 Mbps & 11 Mbps.

RATE SHIFTING

Rate shifting refers the ability of a device to dynamically and automatically change between the various speeds or rate at which data is transmitted. The data rate negotiation process is a dynamic one; the negotiated data rate is subject to change as conditions change. The process

whereby a data rate is established or reestablished is based upon the number of errors received when a packet is sent at a certain data rate using modulation type. If number of received errors passes a certain vendor specified threshold, the Wi-Fi device will take action first. Wi-Fi client will search across all channels in 2.4 GHz band for an access point with a stronger signal. Then it will associate itself with the access point providing the stronger signal and thereby establish or maintain the highest data rate possible. If however the client is unable to find an access point that provides a stronger signal, it will begin the process of rate shifting. This automatic process uses progressively less complex, and therefore more robust, modulation types that will result in fewer errors, greater geographic coverage and a lower data rate.

In general, errors are caused by interference, sometimes caused by competitive source of radio energy and at other times by phenomenon of Multipath.

THROUGHPUT

The data rate represents the speed at which entire packet, inclusive of transaction overhead travels. Additionally, the data rate does not take into account transmission errors that are serious enough to result in a shift to a lower data rate. Finally the notion of the data rate is applicable to the whole of the transmission medium, not to the individual users who are sharing the medium with all other users.

WI-FI SECURITY

Security becomes vitally important when mobile application traverse across wireless networks. [7]-[9]. This is because communication signals are openly available as they propagate outside the controlled area of homes or buildings.

The security attacks in WLAN are,

1. Reconnaissance attacks: It is unauthorized discovery and mapping of systems, services or vulnerabilities. Wireless snooping and packet sniffing are common terms for eaves dropping.

2. Access attacks:

System access in this context refers to the ability of an unauthorized intruder to gain access to a device for which he does not have an account or password.

3. Denial of Service (DOS):

DOS is when an attacker disables or concepts wireless networks, systems or services with the intent of denying the service to the authorized access.

The Different Security Methodologies are,

SERVICE SET IDENTIFIERS (SSID)

The first generation WLAN security depends on a unique SSID and MAC authentication. The SSID is 1-32 character that can be entered on the clients and AP's. Access Points have option such as SSID broadcast and allow any SSID. The features are enabled by default and make it easy to set up a wireless network. Using 'allow any SSID option' lets the AP to access the client with a blank SSID. The SSID broadcast option sends beacon frames, which advertise SSID. Disabling these two options does not secure the network, because a wireless sniffer can easily capture a valid SSID from normal WLAN traffic. SSID cannot be considered as security feature.

MAC AUTHENTICATION

Many vendors implement MAC authentication. Most vendors simply require each AP to have a list of valid MAC address. Some vendors allow AP to have a list of valid MAC addresses. Controlling wireless network access by using MAC address is tedious. MAC addresses are not a real security mechanism because all the MAC addresses are unencrypted when transmitted. An attacker would only need to capture a valid MAC address to gain access over the network with a technique called MAC

spoofing. Address resolution protocol (ARP) is a mandatory network protocol that a sending wireless client uses to discover the MAC address of a destination client.

WIRED EQUIVALENT PRIVACY (WEP)

The IEEE 802.11 standard includes WEP to protect authorized users of a WLAN from casual eaves dropping. The IEEE 802.11 WEP standard specifies a static key. So that it can be exported and used world wide. Most vendors have extended WEP to 128 bit or more. When using WEP, both wireless client and AP must have a matching WEP key. WEP is based on an existing familiar encryption type-Rivest Cipher (RC4).The IEEE 802.11 standard provides the schemes for defining the WEP keys to be used on WLAN.

1.A set of as many as four default keys are shared by all stations, including clients obtain the default keys, it can communicate securely with all other stations in the subsystem. The problem with default key is that when they become widely distributed, they are more likely to be compromised.

2. In second scheme, each client establishes a key mapping relation ship with another station. This is a more secure form of operation, because fewer stations have the keys distributing such as unicast keys, however becomes difficult as the number of stations increases. So, WEP encryption is weak in several ways.

WI-FI PROTECTED ACCESS (WPA)

WPA is an upgrade to WEP that offers dynamic key encryption and mutual authentication. WPA clients utilize different encryption keys that change periodically. This makes it more difficult to crack the encryption. A significant issue of WPA is, it only encrypts packets that travel over the wireless portion of the network. This offers a major security problem when clients are interfacing with the public networks.

VIRTUAL PRIVATE NETWORK (VPN)

The VPN serves as the strong solution, when developing mobile application interfacing with public networks. VPN provides an effective means of end-end encryption. VPN are also effective when clients roam across different types of wireless network because they operate above the dissimilar network connection levels.

Some authentication mechanisms like 802.1x combined with EAP-TLS to counter unauthorized access issues. EAP-TLS is based on the X.509 certificates. TLS requires authentication servers such as RADIUS on network to perform validation.

WI-FI IMPAIRMENTS

Limited throughput, spotty coverage, and radio interference are a few of the problems that will wreak havoc unless you include special countermeasures in your design.

Wireless LAN protocols, for example, induce much more overhead into the transfer of packets than wired networks. In contrast to Ethernet, an IEEE 802.11 ("Wi-Fi") wireless LAN client device or Access Point receiving a packet must always send an acknowledgment to the sending party if no errors are found in the Frame. This is necessary because the sender has no way of discerning if the packet made it through the channel without errors.

In addition, hidden nodes can cause substantial collisions in wireless networks. This occurs when Station A and Station B are sending data to a common destination, and neither Station A nor Station B can hear each other to facilitate taking turns using the air medium. The resulting collisions require both stations to retransmit their data. This problem feeds upon itself with a greater number of active stations. The additional retransmissions that result from the increasing numbers of collisions cause more retransmissions, and so on. This additional overhead of

acknowledgments and retransmissions significantly reduces the available throughput, which is the transfer rate that you can count on when moving real information. An IEEE 802.11b wireless LAN, for example, may deliver 11Mbps connections, but this is the rate that a station will transmit an individual frame of data. After factoring in the overhead, the resulting total throughput is at best 5Mbps. In fact, the total throughput decreases even more as the number of active stations increases. Conserving bandwidth when sending data over a wireless network, start by streamlining the transfer of information. For example, combine smaller data packets into a single larger packet to avoid the extra overhead that each packet requires. This could backfire on you, though, if significant radio interference is present. Larger packets take longer time to transmit, which makes them vulnerable to errors that may results in interference. It is possible, however, to utilize mechanisms that adapt to the interference. Take advantage of compression algorithms at the transport layer to help minimize the number of bits sent over the wireless link. Some implementations of wireless middleware use header compressions, where mechanisms replace traditional packet headers with a much shorter bit sequence before transmission. Some companies do a great job of identifying the optimum location of access points through effective site surveys. The goal is to provide complete coverage in all areas where users may roam.

ADVANTAGES

- Wi-Fi allows LANs to be deployed without cabling. [10]. So, it potentially reduces costs of network deployment and expansion.
- Different bands of access points and client network interface are interoperable at basic level of service.
- Wi-Fi network support roaming, where users can move from one access point to another.
- While connected on a Wi-Fi network, it is possible to move about without breaking the network connection.
- Modern Access Points and Client Cards have excellent in-built security and encryption.

Disadvantages:

- The disadvantage is the use of 2.4 GHz frequency does not require a license in most of the countries.
- The security method adopted (WEP) is easily breakable.

APPLICATIONS

WLAN is applicable in various areas like Health care system, Field Services etc. [11]-[12]. Here we will discuss about Classroom Networking and Warehousing.

WAREHOUSING

Warehouse staff must manage the receiving, putting away, inventory, and picking and shipping of goods. These responsibilities require the staff to be mobile. Warehouse operations have traditionally been a paper-intensive and time-consuming environment. An organization, however, can eliminate paper, reduce errors, and decrease the time necessary to move items in and out by giving each warehouse employee a handheld computing device with a bar code scanner interfaced via a wireless network to a warehouse inventory system.

Upon receiving an item for storage within the warehouse, a clerk can scan the item's bar coded item number and enter other information from a small keypad into the database via the handheld device. The system can respond with a location by printing a put-away label. A forklift operator can then move the item to a storage place and account for the procedure by scanning the item's bar code. The inventory system keeps track of all transactions, making it very easy to produce accurate inventory reports.

As shipping orders enter the warehouse, the inventory system produces a list of the items and their locations. A clerk can view this list from the database via a handheld device and locate the items needed to assemble a shipment. As the clerk removes the items from the storage bins, the database can be updated via the handheld device. All of these functions depend heavily on wireless networks to maintain real-time access to data stored in a central database.

CLASS ROOM NETWORK

In order to facilitate a better teaching environment for students, the campus is equipped with network access points. This means that teaching staff can get access to the campus network and internet while teaching.

Teaching staff can experience similar computer environment in class rooms as the one in lecture theaters by connecting your own notebook to the network access point and to LCD projection panel. The network access points are usually installed near the teaching area. Apart from the traditional use of presentation software in class room, teachers can use internet to help teaching i.e.) accessing various materials on the internet.

CONCLUSION

To conclude Wi-Fi gives the freedom to change locations and give full access to your files in office and network connections where you are. Wi-Fi does better than other technology. Variety of high speed internet connections with a Wi-Fi networking includes cable modems, DSL, where the broad band connection will connect your gateway or access points and its internet connections will de distributed to all computers in the network.

References:

[1] Behrouz A.Forouzan, *"Local Area Networks"*, Tata McGraw-Hill edition 2000, ISBN: 0-07-048666-2

[2] William Stallings, *"Wireless Communication And Networking"*, Pearson Education Asia.

[3] Dr.Kamilo Feher, *"Wireless digital Communications"*, Eastern Economy Edition.

[4] Cisco Systems, *"Fundamentals of Wireless LANs - Companion Guide"*, Pearson Education 2004, ISBN: 81-297-0645-8

[5] www.compnetworking.about.com /cs/wireless/802.11a/aa802.1standard.htm

[6] Neil Reid & RenSeide,*"802.11 (Wi-Fi) Networking Handbooks."* Tata McGraw-Hill Edition 2003, ISBN: 0-07-053143-9

[7] www.oninformation.com/OnInfo2/wi_fi.htm

[8] http://www.wireless-nets.com wireless_lan_papers.htm

[9] www.ieee.org/

[10] http://www.ncexchange.org/

[11] http://www.ust.hk/itsc/network/mobilecomp

[12] wise.dlsu.edu.ph/press-releases/eclassroom.asp