Assignment 1

ITS323

Introduction to Data Communications

Presented by

Group 30

Mr. Kunapong	Unnoi	5222800740
Mr. Plaipetch	Vithayapul	5122792070
Ms. Titima	Wattanachaipong	5122792302

Submitted to

Asst. Prof. Dr. Steven Gordon

8 September 2010

Content

Table of Participation

Section	Mr. Kunapong Unnoi 5222800740	Mr. Plaipetch Vithayapul 5122792070	Ms. Titima Wattanachaipong 5122792302
Wireless LAN	-	-	100
Bluetooth	-	100	-
ZigBee	100	-	-
WiMax	100	-	-

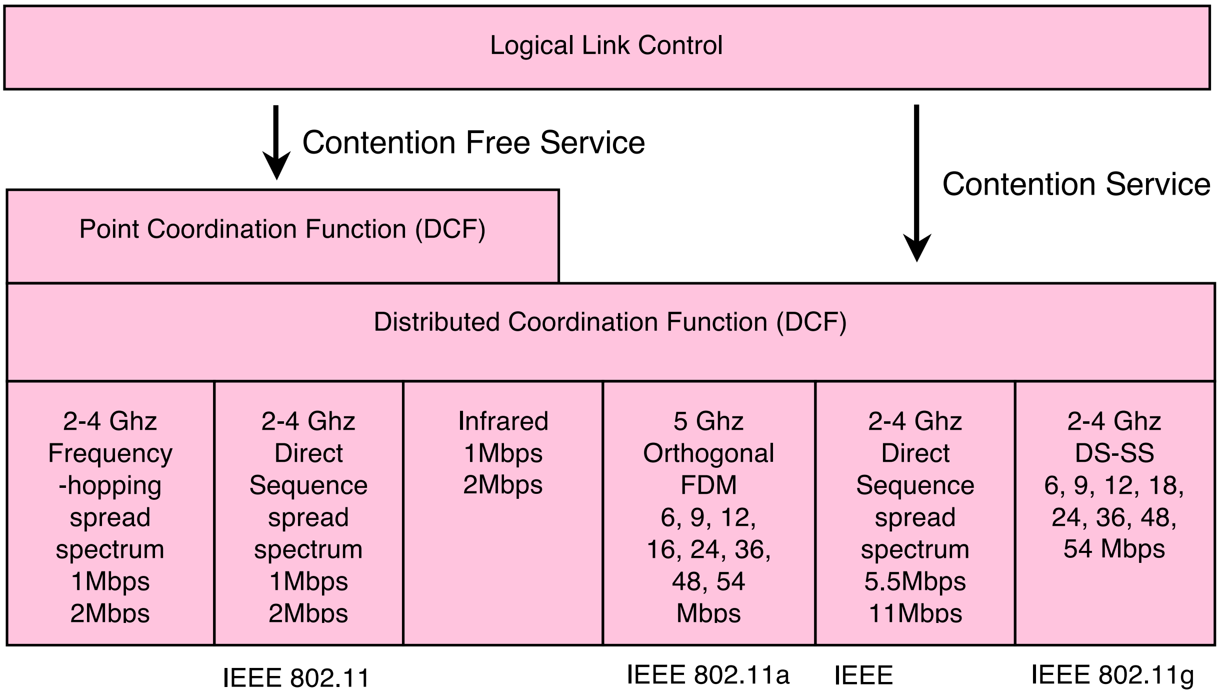
Wireless Local Area Network

Overview

In Computer network a Wireless Local Area Network (WLAN), is a closely grouped system of devices that communicate via radio waves instead of wires. Wireless LAN's typically replace wired computer networks, providing users with more flexibility and freedom of movement within the workplace. Users can access the company intranet or even the World Wide Web from anywhere on the company campus without relying on the availability of wired cables and connection. A wireless LAN (WLAN) is a flexible data communication system implemented as an extension or as an alternative for, a wired LAN within a building or campus. Using electromagnetic waves, WLAN's transmits and receive data over the air, minimizing the need for wired connections. Thus, WLANs combine data connectivity with user mobility

Over the last seven years, WLANs have gained strong popularity in a number of vertical markets. Today WLANs are becoming more widely recognized as a general-purpose connectivity alternative for a broad range of business customers.

Protocol description, Architectures, and protocol stacks.



Logical Link Control

Contention Free Service

Contention Service

Point Coordination Function (DCF)

Distributed Coordination Function (DCF)

2-4 Ghz Frequency -hopping spread spectrum 1Mbps 2Mbps

2-4 Ghz Direct Sequence spread spectrum 1Mbps 2Mbps

Infrared 1Mbps 2Mbps

5 Ghz Orthogonal FDM 6, 9, 12, 16, 24, 36, 48, 54 Mbps

2-4 Ghz Direct Sequence spread spectrum 5.5Mbps 11Mbps

2-4 Ghz DS-SS 6, 9, 12, 18, 24, 36, 48, 54 Mbps

IEEE 802.11

IEEE 802.11a

IEEE

IEEE 802.11g

General Description

802.11 family is over-the-air modulation techniques that use the same basic protocol which has 802.11, 802.11a, 802.11b, 802.11g, and 802.11n the most popular are those defined by the 802.11b and 802.11g protocols. 802.11 was the first wireless networking standard but the first widely accepted one is

802.11b followed by 802.11g and 802.11n. While security was enhanced via the 802.11i. 802.11n is a new multi-streaming modulation technique.

802.11b and 802.11g use the 2.4 GHz ISM band operating which may occasionally suffer interference from microwave ovens, cordless telephones and Bluetooth devices. Both 802.11 and bluetooth control their interference by using spread spectrum modulation. Bluetooth use a frequency hopping spread spectrum signaling method (FHSS), while 802.11b and 802.11g use the direct sequence spread spectrum signaling (DSSS) and orthogonal frequency division multiplexing (OFDM) methods, respectively 802.11a uses the 5 GHz band which offer at least 19 non-overlapping channels. The wireless performance is depending on the environment.

802.11 network standards

Protocol	**Release**	**Freq. (GHz)**	**Bandwidth (MHz)**	**Date rate per stream (Mbit/s)**	**Modulation**	**Approximate indoor range**	**Approximate outdoor range**
						(m)	**(m)**
–	Jun 1997	2.4	20	1, 2	DSSS, FHSS	20	100
a	Sep 1999	5	20	6, 9, 12, 18, 24, 36, 48, 54	OFDM	35	120
		3.7				--	5,000
b	Sep 1999	2.4	20	1, 2, 5.5, 11	DSSS	38	140
g	Jun 2003	2.4	20	1, 2, 6, 9, 12, 18, 24, 36, 48, 54	OFDM, DSSS	38	140
n	Oct 2009	2.4/5	20	7.2, 14.4, 21.7, 28.9, 43.3, 57.8, 65, 72.2[z]	OFDM	70	250
			40	15, 30, 45, 60, 90, 120, 135, 150[z]		70	250

802.11 Modulation Techniques and signal encoding.

Frequency-hopping spread spectrum (FHSS)

In order to be easy to understand FHSS is a method of transmitting radio signals by rapidly switching a carrier among many frequency channels by using random sequence which known to both transmitter and receiver. This method enable 3 advantage over fixed-frequency transmission

1. Spread-spectrum signals are highly resistant to narrowband interference.
2. Spread-spectrum signals are difficult to intercept.

3. Spread-spectrum transmissions can share a frequency band with many types of conventional transmissions with minimal interference. The spread-spectrum signals add minimal noise to the narrow-frequency communications, and vice versa. As a result, bandwidth can be utilized more efficiently.

Algorithm

Typically, the initiation of an FHSS communication is as follows

1.The initiating party sends a request via a predefined frequency or control channel.
2.The receiving party sends a number, known as a seed.
3.The initiating party uses the number as a variable in a predefined algorithm, which calculates the sequence of frequencies that must be used. Most often the period of the frequency change is predefined, as to allow a single base station to serve multiple connections.
4.The initiating party sends a synchronization signal via the first frequency in the calculated sequence, thus acknowledging to the receiving party it has correctly calculated the sequence.
5.The communication begins, and both the receiving and the sending party change their frequencies along the calculated order, starting at the same point in time.

In some uses, most often military, a predefined frequency-hopping sequence is negotiated, and after completing the first step the procedure is continued from number 5.

Orthogonal frequency-division multiplexing (OFDM)

Before going in to OFDM you have to understand what is frequency-division multiplexing (FDM) first. FDM is a form of signal multiplexing which involves assigning non-overlapping frequency ranges to different signals or to each user of a medium. FDM is used as to allow multiple users to share a physical communications channel, it is called frequency-division multiplexing access (FDMA).

OFDM is a FDM scheme utilized as a digital multi-carrier modulation method. A large number of orthogonal sub-carriers are used to carry data. The data is divided into many parallel data streams.

OFDM has developed into a popular scheme for wide band digital communication, whether wireless or over copper wires, used in applications such as digital television and audio broadcasting, wireless networking and broadband internet access. The advantage of OFDM are

- Can easily adapt to severe channel conditions without complex equalization.
- Robust against narrow-band co-channel interference.
- High spectral efficiency as compared to conventional modulation schemes, spread spectrum, etc.
- Efficient implementation using Fast Fourier Transform (FFT).
- Low sensitivity to time synchronization errors.

Protocols

802.11 Legacy

The original version of the standard IEEE 802.11 was released in 1997 and clarified in 1999, but is today obsolete. It specified two net bit rates of 1 or 2 megabits per second (Mbit/s), plus forward error correction code. It specified three alternative physical layer technologies: diffuse infrared operating at 1 Mbit/s; frequency-hopping spread spectrum operating at 1 Mbit/s or 2 Mbit/s; and direct-sequence spread spectrum operating at 1

Mbit/s or 2 Mbit/s. The latter two radio technologies used microwave transmission over the Industrial Scientific Medical frequency band at 2.4 GHz. Some earlier WLAN technologies used lower frequencies, such as the U.S. 900 MHz ISM band.
Legacy 802.11 with direct-sequence spread spectrum was rapidly supplanted and popularized by 802.11b.

802.11a

The 802.11a standard uses the same data link layer protocol and frame format as the original standard, but an OFDM based air interface (physical layer). It operates in the 5 GHz band with a maximum net data rate of 54 Mbit/s, plus error correction code, which yields realistic net achievable throughput in the mid-20 Mbit/s

Since the 2.4 GHz band is heavily used to the point of being crowded, using the relatively unused 5 GHz band gives 802.11a a significant advantage. However, this high carrier frequency also brings a disadvantage: the effective overall range of 802.11a is less than that of 802.11b/g. In theory, 802.11a signals are absorbed more readily by walls and other solid objects in their path due to their smaller wavelength and, as a result, cannot penetrate as far as those of 802.11b. In practice, 802.11b typically has a higher range at low speeds (802.11b will reduce speed to 5 Mbit/s or even 1 Mbit/s at low signal strengths). However, at higher speeds, 802.11a often has the same or greater range due to less interference.

802.11a products started shipping late, due to the slow availability of the harder to manufacture 5 GHz components needed to implement products. First generation product performance was poor and plagued with problems. When second generation products started shipping, 802.11a was not widely adopted in the consumer space because the less-expensive 802.11b was already widely adopted.

However, 802.11a later saw significant penetration into enterprise network environments, despite the initial cost disadvantages, particularly for businesses which required increased capacity and reliability over 802.11b/g-only networks.

With the arrival of less expensive early 802.11g products on the market, which were backwards-compatible with 802.11b, the bandwidth advantage of the 5 GHz 802.11a in the consumer market was reduced. Manufacturers of 802.11a equipment responded to the lack of market success by significantly improving the implementations and by making technology that can use more than one band a standard.

Dual-band, or dual-mode Access Points and Network Interface Cards (NICs) that can automatically handle a and b/g, are now common in all the markets, and very close in price to b/g- only devices.

802.11b

802.11b has a maximum raw data rate of 11 Mbit/s and uses the same media access method defined in the original standard. 802.11b products appeared on the market in early 2000, since 802.11b is a direct extension of the modulation technique defined in the original standard. The dramatic increase in throughput of 802.11b (compared to the original standard) along with simultaneous substantial price reductions led to the rapid acceptance of 802.11b as the definitive wireless LAN technology.

802.11b devices suffer interference from other products operating in the 2.4 GHz band. Devices operating in the 2.4 GHz range include: microwave ovens, Bluetooth devices, baby monitors and cordless telephones.

802.11b Range Coverage

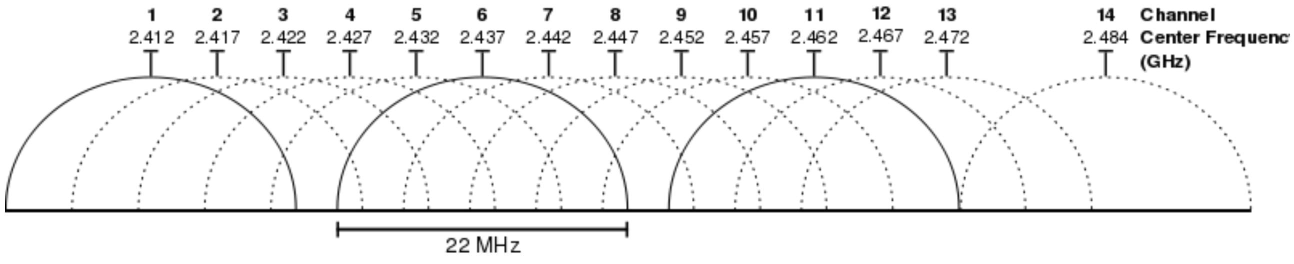
802.11b is used in a point-to-multipoint configuration, an access point communicates via an omni-directional antenna with one or more nomadic or mobile clients that are located in a coverage area around the access point. Typical indoor range is 30 m at 11 Mbit/s and 90 m (300 ft) at 1 Mbit/s. The overall bandwidth is dynamically demand shared across all the users on a channel. With high-gain external antennas, the protocol can also be used in fixed point-to-point arrangements, typically at ranges up to 8 kilometers. This is usually done in place of costly leased lines or very cumbersome microwave communications equipment. Designers of such installations who wish to remain within the law must however be careful about legal limitations on effective radiated power.

802.11b cards can operate at 11 Mbit/s, but will scale back to 5.5, then 2, then 1 Mbit/s, if signal quality becomes an issue.

802.11b/g Channels

802.11b/g frequency map

Channel	Center Frequency	Frequency delta	Channel Width	Overlaps Channels
1	2.412 GHz		2.401–2.423 GHz	2–5
2	2.417 GHz	5 MHz	2.406–2.428 GHz	1,3–6
3	2.422 GHz	5 MHz	2.411–2.433 GHz	1–2,4–7
4	2.427 GHz	5 MHz	2.416–2.438 GHz	1–3,5–8
5	2.432 GHz	5 MHz	2.421–2.443 GHz	1–4,6–9
6	2.437 GHz	5 MHz	2.426–2.448 GHz	2–5,7–10
7	2.442 GHz	5 MHz	2.431–2.453 GHz	3–6,8–11
8	2.447 GHz	5 MHz	2.436–2.458 GHz	4–7,9–12
9	2.452 GHz	5 MHz	2.441–2.463 GHz	5–8,10–13
10	2.457 GHz	5 MHz	2.446–2.468 GHz	6–9,11–13
11	2.462 GHz	5 MHz	2.451–2.473 GHz	7–10,12–13
12	2.467 GHz	5 MHz	2.456–2.478 GHz	8–11,13–14
13	2.472 GHz	5 MHz	2.461–2.483 GHz	9–12,14
14	2.484 GHz	12 MHz	2.473–2.495 GHz	12–13



802.11g

In June 2003, a third modulation standard was ratified: 802.11g. Which works in the 2.4 GHz band, but uses the same OFDM based transmission scheme as 802.11a. It operates at a maximum physical layer bit rate of 54 Mbit/s exclusive of forward error correction codes, or about 22 Mbit/s average throughput. 802.11g hardware is fully backwards compatible with 802.11b hardware and therefore is encumbered with legacy issues that reduce throughput when compared to 802.11a by ~21%.

The then-proposed 802.11g standard was rapidly adopted by consumers starting in January 2003, due to the desire for higher data rates as well as to reductions in manufacturing costs. By summer 2003, most dual-band 802.11a/b products became dual-band/tri-mode, supporting a and b/g in a single mobile adapter card or access point. Details of making b and g work well together occupied much of the lingering technical process; in an 802.11g network, however, activity of an 802.11b participant will reduce the data rate of the overall 802.11g network.

Like 802.11b, 802.11g devices suffer interference from other products operating in the 2.4 GHz band, for example wireless keyboards.

802.11n

IEEE 802.11n is an amendment to all previous 802.11 standards by adding multiple-input multiple-output (MIMO) and 40 MHz channels to the physical layer, and frame aggregation to the MAC layer.

MIMO is a technology which uses multiple antennas to coherently resolve more information than possible using a single antenna. One way it provides this is through Spatial Division Multiplexing (SDM). SDM spatially multiplexes multiple independent data streams, transferred simultaneously within one spectral channel of bandwidth.

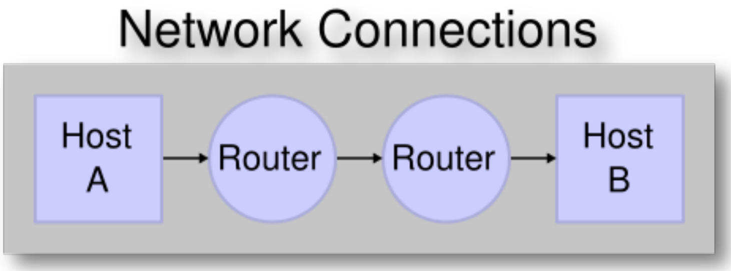
Channels operating at 40 MHz are another feature incorporated into 802.11n which doubles the channel width from 20 MHz in previous 802.11 physical layer to transmit data. This allows for a doubling of the physical data rate over a single 20 MHz channel. It can be enabled in the 5 GHz mode, or within the 2.4 GHz if there is knowledge that it will not interfere with any other 802.11 or non-802.11 (such as Bluetooth) system using those same frequencies.

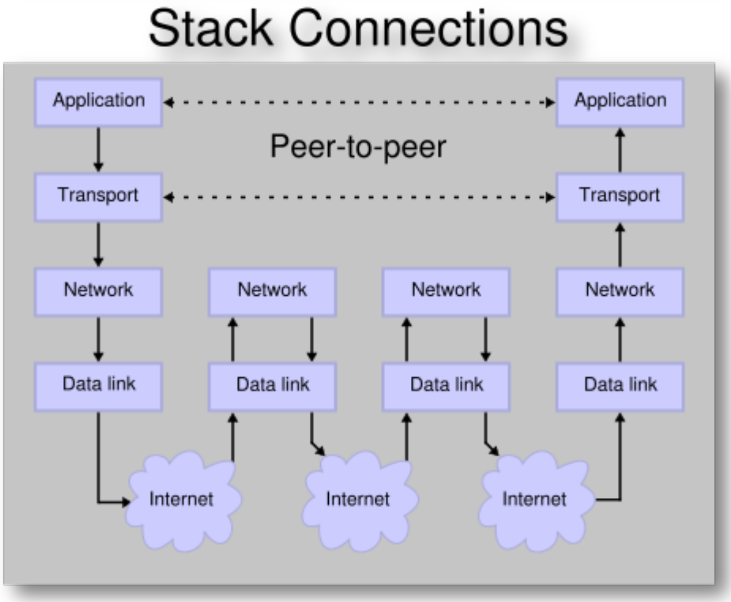
Coupling MIMO architecture with wider bandwidth channels offers increased physical transfer rate over 802.11a (5 GHz) and 802.11g (2.4 GHz).

802.11 Protocol Stack

A protocol stack is a particular software implementation of a computer networking protocol suite. The suite is the definition of the protocols, and the stack is the software implementation of them. Individual protocols within a suite are often designed with a single purpose in mind. This modularization makes design and evaluation easier.

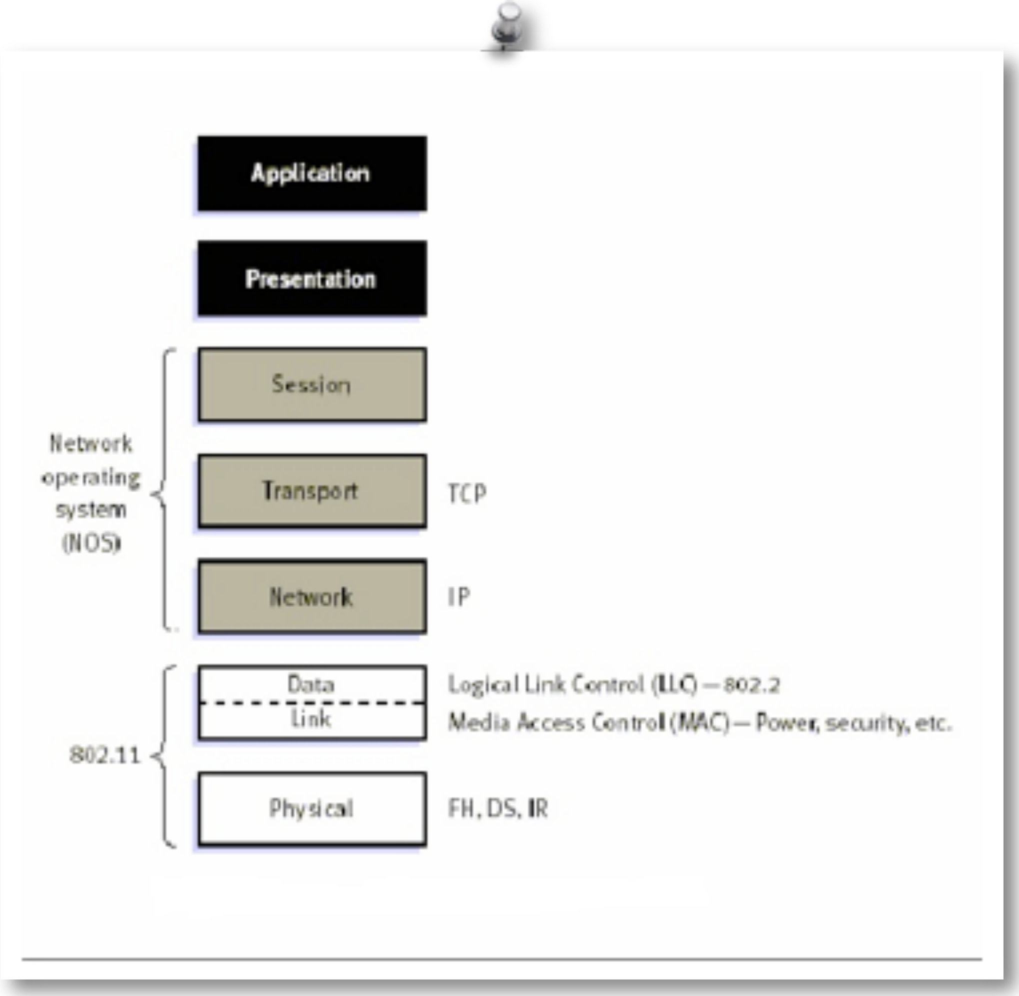
Because each protocol module usually communicates with two others, they are commonly imagined as layers in a stack of protocols. The lowest protocol always deals with "low-level", physical interaction of the hardware. Every higher layer adds more features. User applications habitually deal only with the topmost layers.





The protocols used by all the 802 variants, including Ethernet, have a certain commonality of structure. In the figure we see a partial view of the 802.11 protocol stack. The physical layer corresponds to the OSI physical layer fairly well, but the data link layer in all the 802 protocols is split into two or more sublayers. In 802.11, the MAC sublayer determines how the channel is allocated, that is, and who gets to transmit next.

Above it is the LLC (Logical Link Control) sublayer, whose job it is to hide the differences between the different 802 variants and make them indistinguishable as far as the network layer is concerned. The 802.11 standard specifies three transmission techniques allowed in the physical layer. The infrared method uses much the same technology as television remote controls do. The other two use short-range radio, using techniques called FHSS and DSSS. Both of these use a part of the spectrum that does not require licensing (the 2.4-GHz ISM band). Radio-controlled garage door openers also use this piece of the spectrum, so notebook computer may find itself in competition with your garage door. Cordless telephones and microwave ovens also use this band.


Application
Presentation
Session
Transport
Network
Data
Link
Physical
Network operating system (NOS)
802.11
TCP
IP
Logical Link Control (LLC) — 802.2
Media Access Control (MAC) — Power, security, etc.
FH, DS, IR

Transmit Power

The spectrum regulatory body of each country restricts signal power levels of various frequencies to accommodate needs of users and avoid RF interference. Most countries deem 802.11 wireless LANs as license free. In order to qualify for license free operation, however, the radio devices must limit power levels to relatively low values.

In most situation user would prefer to use high transmit power to increase the range of access points. The problem is that wireless signal interference with other nearby equipment would occur more often. So we must control the amount of power must we use.

The gain of an antenna represents how well it increases effective signal power in a particular direction, with dBi as the unit of measure represents the gain of an antenna.

Manufacturers determine the antenna's dBi value, so it's a relief we don't have to calculate it. What we do need to know is that every three dBi doubles the power of a wireless signal. As a result, higher values of dBi extend the range of a wireless LAN.

A typical indoor WLAN consists of enough access points to cover the facility to enable wireless mobility for users. Access points generally have omni-directional antennas that propagate signal in most directions, which maximizes connectivity for mobile applications. When using omni-directional antennas having less than 6 dB gain in this scenario, the FCC rules require EIRP to be 1 watt (1,000 milliwatts) or less.

User can set the transmit power in an 802.11a/b/g/n access point or client to its highest level (generally 100 milliwatts) and use a typical 3 dB omni-directional antenna. This combination results in only 200 milliwatts EIRP, which is well within FCC regulations.

Reference : U.S., the FCC (Federal Communications Commission)

Fragmentation and receive thresholds

The fragmentation threshold establishes the level that traffic fragments. When an AP sends a transmission, the traffic fragments into smaller pieces. Smaller frames result in fewer collisions. When the station receives those pieces, it sends an acknowledgement to the AP. Pieces that are not received are resent. The benefit is that with more pieces sent, there is a better chance that the entire data transmitted is received. The downside is obvious, more fragmentation means more throughput consumed with acknowledgement messages.

A good rule of thumb for the fragmentation threshold setting is that if few collisions are occurring (less than 5 percent), don't use fragmentation. The extra overhead created by the headers reduces throughput.

On the other hand, if you see a good deal of collisions, you can attenuate them, set the fragmentation threshold to around 1000 bytes, and adjust it up or down from there. User have to strike a balance between throughput and collisions.

You can set the fragmentation threshold between 256 and 2346 bytes. The default setting is 2338 bytes and can be adjusted up or down.

Antenna

Antenna is a thing that transmits or receives electromagnetic waves. In other words, antennas convert electromagnetic radiation into electrical current, or vice versa. Antennas generally deal in the transmission and reception of radio waves, and are a necessary part of all radio equipment. Antennas are used in systems such as radio and television broadcasting, point-to-point radio communication, **wireless LAN**,etc.

Typically in wireless LAN devices such as wireless router or wireless access point usually use stick shape antenna and newly model comes with more than 1 antenna as figure show below. In wireless LAN card in every laptop comes with flat antenna printed on the card in practical it will effect on signal strength.

Distance and range of usage

Wireless networks have limited range. A typical wireless router using 802.11b or 802.11g with a stock antenna might have a range of 32 m indoors and 95 m outdoors. The IEEE 802.11n can exceed that range by more than two times. Range also varies with frequency band. Wi-Fi in the 2.4 GHz frequency block has slightly better range than Wi-Fi in the 5 GHz frequency block. Outdoor ranges - through use of directional antennas - can be improved with antennas located several kilometers or more from their base. The maximum amount of power that a Wi-Fi device can transmit is limited by local regulations. Wireless LAN (Wi-Fi) has fairly high power-consumption compared to some other standards. Technologies such as Bluetooth provide a much shorter propagation range of <10m and in general have a lower power-consumption. Other low-power technologies such as ZigBee have fairly long range, but much lower data rate. The high power-consumption of Wi-Fi makes battery life in mobile devices a concern.

Applications

What scenarios/applications are they intended for ?

Wireless local area network (WLAN) is intended to create an area of network for users to communicate and access to internet, for example home network, office network, coffee shop Wi-Fi. Today you can share media contents among family member, streaming internet from your TV. In addition WLAN is new technology that will replace Local Area Network. The major advantage of WLAN is user mobility, easy access, easy setup but it also contain some disadvantage like security. Because wireless network traffic transmit over the air anyone could received and look in to transmitted data.

How would the technology be used by a typical user ?

Since WLAN is very easy to install, in practical user just unpack, plug in and its ready to use. Anyone could use this technology wherever they want to create small area of network. In some cases if user want to use in huge area such as 3 or more floor building user may have to setup mesh network in order to improve signal coverage.

What types of devices are required ?

In order to use WLAN transmitted device and received device must be prepared. In this case one WLAN component such as router, Wi-Fi card can act as transmitter and/or receiver for example ad-hoc or base station mode. Briefly if user require to create Wireless networks they need to have at least 2 devices that can transmit and received data.

Usage

Are they being used extensively in Thailand ? Other countries ? Why not ?

In Thailand wireless-LAN is being use widely, the oblivious example is Truemove which is internet provider that gives user a service to connect to internet via TrueWifi networks around Bangkok. The same case apply to KSC internet and 3BB hotspot around Bangkok metropolis. Also this method is one of the most way that home user in Thailand are using now a days.

Cost

What is the app ost of the equipment ? What other costs are associated with using the technology ?

To setup wireless LAN at least you need 1 wireless access point which is about 2,000 – 3,000 baht. If your devices such as PC is not support Wi-Fi networks you have to use additional wireless USB which cost about 700 – 1,000 Baht depend on features and manufacturer. Also the cost of the equipment can’t be fix, if user need to setup wireless LAN in large area user may need to use extra access point or larger, taller antennas.

ZIGBEE technology

Introduction to zigbee

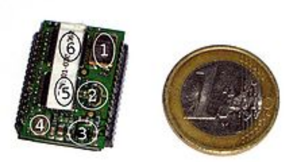
ZigBee is a specification for a suite of high level communication protocols using small, low-power digital radios based on the IEEE 802.15.4-2003 standard for wireless home area networks (WHANs), such as wireless light switches with lamps, electrical meters with in-home-displays, consumer electronics equipment via short-range radio. The technology defined by the ZigBee specification is intended to be simpler and less expensive than other WPAns, such as Bluetooth. ZigBee is targeted at radio-frequency (RF) applications that require a low data rate, long battery life, and secure networking.

ZigBee applications include:

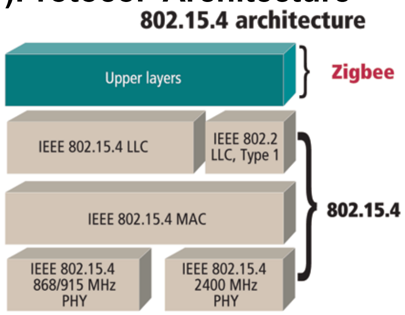
- Home and office automation
- Industrial automation
- Medical monitoring
- Low-power sensors
- HVAC control
- Plus many other control and monitoring uses

ZigBee targets the application domain of low power, low duty cycle and low data rate requirement devices.

Example of zigbee:



1)Protocol Architecture



Divide into 3 layer :

Physical Layer: The physical layer ultimately provides the data transmission service, as well as the interface to the physical layer management entity, which offers access to every layer management function and maintains a database of information on related personal area networks. Thus, physical manages the physical RF transceiver and performs channel selection and energy and signal management functions.

MAC Layer: The medium access control (MAC) allows the transmission of MAC frames through the use of the physical channel. Besides the data service, it offers a management interface and itself manages access to the physical channel and network beaconing. It also controls frame validation, guarantees time slots and handles node associations. Finally, it offers hook points for secure services.

Higher Layer: Other higher-level layers and interoperability sublayers are not defined in the standard. There exist specifications, such as ZigBee, which build on this standard to propose integral solutions. TinyOS, Unison RTOS and DSPnano RTOS stacks also use a few items of IEEE 802.15.4 hardware.

2)Data Transmission

2.1) Spectrum: uses DSSS [Direct Sequence Spread Spectrum], which divides the 2.402 – 2.480 GHz [Giga Hertz] spectrum into 16 channels or 10 channels in the 915 MHz [Mega Hertz] spectrum and 1 channel in the European 868 MHz spectrum.

2.2) Frequency: A new frequency synthesizer with low-power and short settling time is introduced. With two-point channel controls for an integer-N PLL, we have achieved a near zero settling time for any frequency change in 2.4GHz ZigBee band.

2.3) Bandwidth: requiring 5 MHz of bandwidth

2.4) Data Rate: Data rates of 250 kbps (@2.4 GHz), 40 kbps (@ 915 MHz), and 20 kbps (@868 MHz)

3) Transmission Media

3.1) Transmission Power : The transmission power is 0 dBm.(Low power consumption)

3.2) Antennas : Some of the regulatory testing is performed as radiated tests, and the gain of the antenna at the frequency
of interest becomes a factor in the measurements. Gain for an embedded antenna can vary considerably,
from less than –5 dBi to more than 5 dBi, even on simple antennas. This could result in more than 10 dB
of difference from one design or layout to another, even for an identical transmitter.

3.3) Distance : rang of 10-75 meter.

4) Signal Encoding Techniques: ZigBee is use with IEEE802.15.4 in lower layer. Higher Layer was controlled by ZigBee Alliance. The data will send to the end device which is connect with the router. End device can be RFD and FFD. End device can only receive and transmit the data. Router is in the middle stage. It received the data or signal from server and send them to the end device.

5)Error

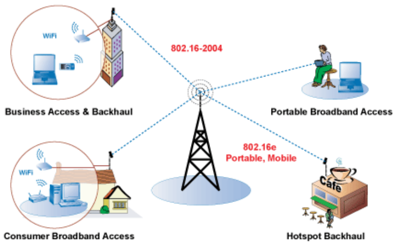
5.1) Error Detection & Error Correction: It does not have error detection in zigbee but use the “ACK” in mac layer that will not happen the error in zigbee

Wimax Technology

Wimax Introduction

WiMax (Worldwide Interoperability for Microwave Access) is a wireless broadband technology, which supports point to multi-point (PMP) broadband wireless access. WiMax is basically a new shorthand term for IEEE Standard 802.16, which was designed to support the European standards. 802.16's predecessors (like 802.11a) were not very accommodative of the European standards, perse.

The IEEE wireless standard has a range of up to 30 miles, and can deliver broadband at around 75 megabits per second. This is theoretically, 20 times faster than a commercially available wireless broadband. The 802.16, WiMax standard was published in March 2002 and provided updated information on the Metropolitan Area Network (MAN) technology. The extension given in the March publication, extended the line-of-sight fixed wireless MAN standard, focused solely on a spectrum from 10 GHz to 60+ GHz. This extension provides for non-line of sight access in low frequency bands like 2 - 11 GHz. These bands are sometimes unlicensed. This also boosts the maximum distance from 31 to 50 miles and supports PMP (point to multipoint) and mesh technologies. The IEEE approved the 802.16 standards in June 2004, and three working groups were formed to evaluate and rate the standards. WiMax can be used for wireless networking like the popular WiFi. WiMax, a second-generation protocol, allows higher data rates over longer distances, efficient use of bandwidth, and avoids interference almost to a minimum. WiMax can be termed partially a successor to the Wi-Fi protocol, which is measured in feet, and works, over shorter distances.


WiFi
802.16-2004
Business Access & Backhaul
Portable Broadband Access
802.16e
Portable, Mobile
WiFi
Café
Consumer Broadband Access
Hotspot Backhaul

1)Protocol Architecture : divided into 2 main layer.

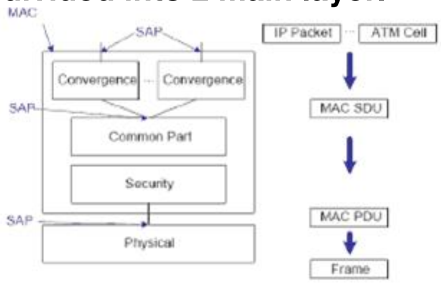


Figure 1: WiMax/802.16 layered architecture [1]

1.1) OSI Physical Layer

- Physical and Transmission The physical Layer establishes the physical connection between both sides, often in the two directions (uplink and downlink). As 802.16 is evidently a digital technology, the physical Layer is responsible for transmission of the bit sequences. It defines the type of signal used, the kind of modulation and demodulation, the transmission power and also other physical characteristics.

1.2) OSI Data Link Layer

- Medium Access Control (MAC):

For transmission , combine data into a frame with address and error detection fields.

For reception , not combine frame, and perform address recognition and error detection.

- Convergence : we can call as CS, is the top sublayer of the MAC Layer in WiMAX/802.16 (Figure 7.1). The CS accepts higher-layer PDUs from the higher layers and transmits them to the MAC CPS where classical type MAC procedures are applied . Classifying and mapping the MSDUs into appropriate CIDs (Connection IDentifier) made by the CS are basic functions of the QoS mechanisms of WiMAX/802.16. Among other functions of the CS is the optional Payload Header Suppression (PHS), the process of suppressing repetitive parts of payload headers at the sender and restoring the headers at the receiver. The classification and mapping made by a QoS management module allow full advantage to be taken of the different Physical layer.

2)Data Transmission

2.1) spectrum : There is no uniform global licensed spectrum for WiMAX, however the WiMAX Forum has published three licensed spectrum profiles: 2.3 GHz, 2.5 GHz and 3.5 GHz, in an effort to drive standardisation and decrease cost.

2.2) frequency The IEEE 802.16 WiMAX standard allows data transmission using multiple broadband frequency ranges. The original 802.16a standard specified transmissions in the range 10 - 66 GHz, but 802.16d allowed lower frequencies in the range 2 to 11 GHz. The lower frequencies used in the later specifications means that the signals suffer less from attenuation and therefore they provide improved range and better coverage within buildings. This brings many benefits to those using these data links within buildings and means that external antennas are not required.

Different bands are available for WiMAX applications in different parts of the world. The frequencies commonly used are 3.5 and 5.8 GHz for 802.16d and 2.3, 2.5 and 3.5 GHz for 802.16e but the use depends upon the countries.

2.3) bandwidth : WiMAX has a theoretical maximum bandwidth of 75Mbps. This bandwidth can be achieved using 64QAM 3/4 modulation. 64QAM can only be utilized under optimal transmission conditions. WiMAX supports the use of a wide range of modulation algorithms to enable the most bandwidth to be realized under all conditions.

2.4) data rate : Wimax able to provide data rates of up to 75 Mbps and as a result it is ideal for fixed, DSL replacement applications. It may also be used for backhaul where the final data may be distributed further to individual users. Cell radii are typically up to 75 km.

3) Transmission Media

3.1) Transmission Power :

- For base station is +43 dBm
- For mobile station is +23 dBm.

3.2) Antennas : Use multi-antennas for wimax technology (MIMO = multiple input multiple output)

3.3) Distance : Range of **30 miles** (50 km) with wireless access. The increased range is due to the frequencies used and the power of the transmitter.

4) Signal Encoding Techniques

4.1) Analog : The analog signal that sending like a wave and it continue all the time we have to encode the signal into the right analog signal that will be get the right information.

4.2) Digital Data: The information that have the signal not continue for the digital will consist of digital base 2

4.3) Signals: The data and information will exchange between receiver and deliver must chang in to the signal before sending the information

5) Errors

5.1) Error Detection **WiMAX technology** have built-in **error detection techniques** to reduce the system Signal to Noise Ratio (SNR) obligations. Convolutional Encoding, Strong Reed Solomon FEC, and interleaving algorithms are used to identify and correct errors to enhance throughput. These strong error correction techniques assist to recover corrupted frames that may have been missing due to frequency selective fading or burst errors.

5.2) Error Correction: Help to detect and fix the wrong bits while sending the data that decrease the level of data into signal to noise ratio that will help to connect the data that for detect and fix the wrong bits with the real data. For the receiver will calculate the receive and compare the data with error correction bits that make the receiver can check which bits is wrong and try to fix it. But for use the error correction in error correction bits that adding is not pack data for use that call over head so the speed in send the data will be decrease for overhead.

5.3) ARQ use to remove the errors, Automatic Repeat Request (ARQ) is used that cannot be corrected by the Forward **Error Detection** (FEC) by resending the error-ed information again. This notably improves the Bit Error Rate (BER) performance for a similar maximum level.

Bluetooth

“Bluetooth” the truth is the name of the king of Denmark , that be known that "Harald Bluetooth" . During year , A.C. 940-981 is or , about 1,000 ago he get govern Denmark country and the Norway in the age of wiking and want to total up the country to be single. Besides, he is a leader takes the Christianity reaches Denmark country as well. And for the recall the king Bluetooth who the king of Denmark. Which now is leader group in the sense of mobile phone production feeds to the world market. And the “ Bluetooth“ systemis built for apply to a mobile phone , and initial from the country in zone too.

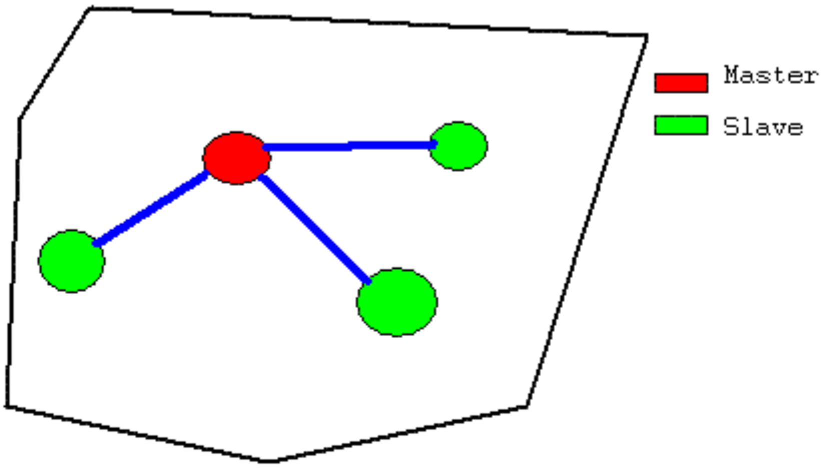
1994, Erecson mobile comunication is estabished by the combination of big companys that is Ericsson, Nokia, IBM, Toshiba and Intel.In the group that use the name “Special Interest Group (SIG)” which in the group will compose the leader mobile phone group and computer etc. Which these group has assessed that in 2002, in the communication tool , the utensil and computer will be set up Bluetooth to use link up between equipments extensively. By in the same year these company has a combination notice and invite other company to attend by bring this technology to use. In year 1999 has spreads the revelation Bluetooth specification Version 1.0 and get more member that are Microsoft, Lucent, 3Com, Motorola.

Bluetooth is a telecommunications industry specification that describes how mobile phones, computers, and personal digital assistants (PDAs) can be easily interconnected using a short-range wireless connection. Using this technology, users of cellular phones, pagers, and personal digital assistants can buy a three-in-one phone that can double as a portable phone at home or in the office, get quickly synchronized with information in a desktop or notebook computer, initiate the sending or receiving of a fax, initiate a print-out, and, in general, have all mobile and fixed computer devices be totally coordinated.

How Bluetooth Works

How Bluetooth cuts the cord

Bluetooth is a curious sounding wireless networking standard that solves the problem of last-inch connectivity. Let's face it, there are lots of standards for last-mile connectivity including DSL, Cable Modem Internet, PON (Passive Optical Networks), T1, BPL (Broadband over Power Line), and even Wi-Fi. Well, Wi-Fi is really more of a last-foot connectivity solution designed to eliminate Ethernet wiring within a home or office. Bluetooth is more likely to eliminate USB and parallel printer cables within a room. It also eliminates other short wires, such as the tiny but annoying cable that links a headset to a cellular phone.



A Piconet

Bluetooth really is a networking standard. Instead of a LAN or Local Area Network, it's a PAN or Personal Area Network. Bluetooth devices establish that are known as piconets. A piconet has a minimum of two devices and a maximum of eight. No manual is needed. The process of setting up the network is completely automatic when Bluetooth enabled devices are within range of each other. One device assumes the role of the master and invites other nearby Bluetooth enabled devices to join the net as slaves. Once all 8 available slots are filled, no other device can join. The master and the slaves take turns communicating in a round-robin scheme. Communications between slaves must be sent via the master and not directly.

All of this is going on at a data rate of 1 Mbps for the standard Bluetooth and up to 3 Mbps for Bluetooth version 2.0. They are compatible standards and run at a speed that the slowest device in the piconet can keep up with. Deducting overhead in the transmission protocol, the basic communications rate is around 720 Kbps. There are options including half-duplex, full duplex, asynchronous connectionless and synchronous connection oriented links. The data bits can be information, digital control words or even two-way audio at 64Kbps. That's perfect for telephone applications, as 64Kbps is the legacy standard for toll quality digitized voice.

Bluetooth operates smack in the middle of the unlicensed 2.4 GHz ISM (Industrial, Scientific and Medical) band. If that has a familiar ring, it's because Wi-Fi uses the same frequencies. What keeps them from clashing is different modulation schemes. Bluetooth deliberately picked a frequency hopping scheme to avoid interfering or being interfered with. It switches randomly among 79 channels at a rate of 1,600 times per second. Only devices on a particular piconet are synchronized to hop to the same frequencies at the same time. This greatly reduces the chances of noise or other transmitters blocking out the entire data stream. If bits are lost on one channel, they can be resent on another.

What are typical uses for Bluetooth?

A popular application is wireless headsets for cell phones. If your phone has Internet capability, a Bluetooth piconet can be established between your phone and nearby laptop computer to give the computer Internet access as well. Bluetooth enabled printers can print pictures from a cell phone or camera that has Bluetooth without needing any wires. Likewise, a Bluetooth enabled PDA can synchronize with a Bluetooth-enabled cell phone, laptop or desktop computer. As devices that meet the 2.0 standard become more commonly available, the higher throughput will be used for wireless audio components and appliances as well. It seems likely that Bluetooth will replace infrared links that need direct line of site and perhaps the bulk of interface cables we're so accustomed to.

Chasing away your wireless blues

Bluetooth is a cable replacement technology, designed to connect paired devices within 10 meters of each other. Given limited range and application, many incorrectly discount Bluetooth as a serious business threat. But new Bluetooth devices can reach up to 100 meters, using internal antennas. Most are promiscuous by default, responding to pages, service discovery probes, and connect requests from anyone. And many harbor security programming flaws associated with the Bluetooth Object Exchange (OBEX) protocol. This has fostered development of new attacks that exploit Bluetooth, such as:

use

List of applications

- Wireless control of and communication between a mobile phone and a handsfree headset. This was one of the earliest applications to become popular.
- Wireless networking between PCs in a confined space and where little bandwidth is required.
- Wireless communication with PC input and output devices, the most common being the mouse, keyboard and printer.
- Transfer of files, contact details, calendar appointments, and reminders between devices with OBEX.
- Replacement of traditional wired serial communications in test equipment, GPS receivers, medical equipment, bar code scanners, and traffic control devices.
- For controls where infrared was traditionally used.
- For low bandwidth applications where higher USB bandwidth is not required and cable-free connection desired.
- Sending small advertisements from Bluetooth-enabled advertising hoardings to other, discoverable, Bluetooth devices.
- Wireless bridge between two Industrial Ethernet (e.g., PROFINET) networks.
- Three seventh-generation game consoles, Nintendo's Wii and Sony's PlayStation 3 and PSP Go, use Bluetooth for their respective wireless controllers.
- Dial-up internet access on personal computers or PDAs using a data-capable mobile phone as a wireless modem like Novatel mifi.
- Short range transmission of health sensor data from medical devices to mobile phone, set-top box or dedicated telehealth devices.
- Allowing a DECT phone to ring and answer calls on behalf of a nearby cell phone
- Real-time location systems (RTLS), are used to track and identify the location of objects in real-time using “Nodes” or “tags” attached to, or embedded in the objects tracked, and “Readers” that receive and process the wireless signals from these tags to determine their locations

Computer requirements

A personal computer that does not have embedded Bluetooth can be used with a Bluetooth adapter or "dongle" that will enable the PC to communicate with other Bluetooth devices (such as mobile phones, mice and keyboards). While some desktop computers and most recent laptops come with a built-in Bluetooth radio, others will require an external one in the form of a dongle.

Unlike its predecessor, IrDA, which requires a separate adapter for each device, Bluetooth allows multiple devices to communicate with a computer over a single adapter.

Operating system support

For more details on this topic, see Bluetooth stack.

Apple has supported Bluetooth since Mac OS X v10.2 which was released in 2002.

For Microsoft platforms, Windows XP Service Pack 2 and SP3 releases have native support for Bluetooth 1.1, 2.0 and 2.0+EDR. Previous versions required users to install their Bluetooth adapter's own drivers, which were not directly supported by Microsoft. Microsoft's own Bluetooth dongles (packaged with their Bluetooth computer devices) have no external drivers and thus require at least Windows XP Service Pack 2. Windows Vista RTM/SP1 with the Feature Pack for Wireless or Windows Vista SP2 support Bluetooth 2.1+EDR. Windows 7 supports Bluetooth 2.1+EDR and Extended Inquiry Response (EIR).

The Windows XP and Windows Vista/Windows 7 Bluetooth stacks support the following Bluetooth profiles natively: PAN, SPP, DUN, HID, HCRP. The Windows XP stack can be replaced by a third party stack which may support more profiles or newer versions of Bluetooth. The Windows Vista/Windows 7 Bluetooth stack supports vendor-supplied additional profiles without requiring the Microsoft stack to be replaced.

Linux has two popular Bluetooth stacks, BlueZ and Affix. The BlueZ stack is included with most Linux kernels and was originally developed by Qualcomm. The Affix stack was developed by Nokia. FreeBSD features Bluetooth support since its 5.0 release. NetBSD features Bluetooth support since its 4.0 release. Its Bluetooth stack has been ported to OpenBSD as well.

Mobile phone requirements

A Bluetooth-enabled mobile phone is able to pair with many devices. To ensure the broadest support of feature functionality together with legacy device support, the Open Mobile Terminal Platform (OMTP) forum has published a recommendations paper, entitled "Bluetooth Local Connectivity".

BLUETOOTH SECURITY

Aside from defining policies, another major concern as Bluetooth starts to plant its foot firmly in the enterprise is its potential to open up security holes. Bluetooth still has questionable security, according to security expert Lisa Phifer, with a host of attacks -- including Bluejacking, Bluesnarfing, Bluebugging and BlueSniper Rifle -- that can intercept data or plant malicious code. There are dozens of Bluetooth attacks, and most embedded Bluetooth devices will just be enabled in a promiscuous discovery mode, with default or no PIN. While it is true that one must be relatively close to a Bluetooth device to connect to it, there are many business situations in which that will be true. Phifer said its proliferation and the potential for attack should be enough to open a few eyes and draw network managers' attention.

Those management programs include everything from enforcing how users set and use device security, to which applications are allowed to run on which devices. IT shops already manage tools to disable other devices, such as digital cameras, games and media players, so adding a Bluetooth-specific set of policies shouldn't present much of a challenge to cut down on security risks and unauthorized use. The challenge comes, however, when it's time to define the policies designed to control Bluetooth. Bluetooth's alliance with UWB could boost its use in the enterprise, but he thinks its core uses will remain in cell phones and other personal device connections that use USB wiring.

Making the best of Bluetooth security

Bluetooth specifications include basic link security measures. By default, most Bluetooth devices operate in unprotected "non-secure" mode. Two additional modes are defined: mode 3 secures the entire wireless link, while mode 2 leaves security up to each authorized application. For best results, use mode 3 to enforce link authentication and encryption for all Bluetooth traffic, and discourage or ban business use of devices that support only mode 1.

When link security is enabled, Bluetooth devices must complete an initial "bonding" exchange to derive pairwise link authentication and encryption keys. The user must give both devices the same PIN code, which is then mixed with a factory-defined unit key. But this pairing process can be compromised by use of weak or predictable PIN codes. To reduce risk, devices should be paired in a private location, using a long, random PIN code. Avoid default PIN codes, easily guessed PIN codes ("0000") and devices that do not support configurable PIN codes.

After bonding, paired Bluetooth devices associate to each other whenever they want to exchange data. As each connection is established, devices exchange challenge-response messages to demonstrate possession of the link key created during bonding. However, this authentication exchange is vulnerable to key-guessing, where a device repeatedly tries to authenticate by trial and error. Active attacks are discouraged by increasing the interval between attempts, but the Bluetooth specification does not enforce a maximum number of attempts. One-way authentication is also vulnerable to a man-in-the-middle attack. To reduce risk, always require authentication on both devices. Where possible, configure Bluetooth products so that users must accept incoming connection requests.

Depending on the negotiated encryption mode, an 8- to 128-bit encryption key can be used to scramble data sent over the link. For best results, avoid encryption mode 1 (no encryption), choosing either mode 2 (encrypt unicast but not broadcast traffic) or better yet mode 3 (encrypt all traffic). Because data that has been encrypted with a too-short key can be analyzed to decrypt captured traffic, both devices should be configured to require 128-bit encryption keys.

Further steps to make best use of these built-in Bluetooth measures include:

- Turn off Bluetooth interfaces when not in use, and disable Bluetooth's discovery feature, whereby each device announces itself to all nearby devices. These common-sense practices reduce the window of opportunity for Bluetooth attacks.
- Configure Bluetooth devices to use the lowest power that meets business needs. Class 3 devices transmit at 1 mW and cannot communicate beyond 10 meters, while class 1 devices transmit at 100 mW to reach up to 100 meters. Adjusting power does not eliminate outsider attack, but it can reduce that possibility.
- Because link keys are stored on paired Bluetooth devices, password protect both devices to prevent use of lost/stolen units. If possible, do not permanently store the pairing PIN code on Bluetooth devices.

To defend against such attacks, combine the good configuration choices and practices described above with Bluetooth product assessment, patching and security auditing.

Audit the airwaves inside your facility to locate all Bluetooth capable devices. For example, walk the halls with a portable Bluetooth scanner like AirDefense Inc.'s BlueWatch, AirMagnet Inc.'s BlueSweep, Berkeley Varitronics Systems Inc.'s Mantis Bluetooth, or Network Chemistry Inc.'s RFprotect BlueScanner. Bear in mind that you'll need to be within 10 meters to detect class 3 devices, and those that have discovery disabled will be harder to spot. Alternatively, enterprises with full-time Wi-Fi intrusion detection (IDS) or intrusion prevention systems (IPS) may detect Bluetooth as a non-descript source of Wi-Fi interference or by fingerprinting individual Bluetooth devices (e.g., Red-M Group Ltd.'s Red-Mobile, AirMagnet Spectrum Analyzer).

Inventory all discovered devices with Bluetooth interfaces, including hardware model, OS, and version. Then search Bluetooth vulnerability and exposure databases (e.g., Trifinite, WVE) to determine whether those devices harbor known issues. For example, Nokia Corp. and Sony Ericsson Mobile Communications AB have issued updates for Bluetooth-capable phones that are vulnerable to Bluesnarfing and BlueBugging. Apply available patches to correct those bugs and retire older devices for which critical patches are unavailable.

Finally, define security policies for all Bluetooth-capable devices that impact your business. This frequently includes handheld devices owned by employees. Here, user education can go a long way toward promoting safer use. Once they learn the potential impact on personal and corporate data, employees are more likely to voluntarily comply with defined policies. They may even welcome configuration assistance, so long as Bluetooth security does not inhibit authorized use. However, where security is truly important, compliance for Bluetooth and other security measures should be enforced through a centrally-administered device management system (e.g., Credant Technologies

Inc.'s Mobile Guardian). After all, link security is part of a much bigger picture -- multi-layered defenses must work together to safeguard Bluetooth devices and their data.

Specifications and features

Bluetooth v1.0 and v1.0B

Versions 1.0 and 1.0B had many problems, and manufacturers had difficulty making their products interoperable. Versions 1.0 and 1.0B also included mandatory Bluetooth hardware device address (BD_ADDR) transmission in the Connecting process (rendering anonymity impossible at the protocol level), which was a major setback for certain services planned for use in Bluetooth environments.

Bluetooth v1.1

- Ratified as IEEE Standard 802.15.1-2002
- Many errors found in the 1.0B specifications were fixed.
- Added support for non-encrypted channels.
- Received Signal Strength Indicator (RSSI).

Bluetooth v1.2

This version is backward compatible with 1.1 and the major enhancements include the following:

- Faster Connection and Discovery
- *Adaptive frequency-hopping spread spectrum (AFH)*, which improves resistance to radio frequency interference by avoiding the use of crowded frequencies in the hopping sequence.
- Higher transmission speeds in practice, up to 721 kbit/s, than in 1.1.
- Extended Synchronous Connections (eSCO), which improve voice quality of audio links by allowing retransmissions of corrupted packets, and may optionally increase audio latency to provide better support for concurrent data transfer.
- Host Controller Interface (HCI) support for three-wire UART.
- Ratified as IEEE Standard 802.15.1-2005
- Introduced Flow Control and Retransmission Modes for L2CAP.

Bluetooth v2.0 + EDR

This version of the Bluetooth Core Specification was released in 2004 and is backward compatible with the previous version 1.2. The main difference is the introduction of an Enhanced Data Rate (EDR) for faster data transfer. The nominal rate of EDR is about 3 megabits per second, although the practical data transfer rate is 2.1 megabits per second. EDR uses a combination of GFSK and Phase Shift Keying modulation (PSK) with two variants, π/4-DQPSK and 8DPSK. EDR can provide a lower power consumption through a reduced duty cycle.

The specification is published as "Bluetooth v2.0 + EDR" which implies that EDR is an optional feature. Aside from EDR, there are other minor improvements to the 2.0

specification, and products may claim compliance to "Bluetooth v2.0" without supporting the higher data rate. At least one commercial device states "Bluetooth v2.0 without EDR" on its data sheet.

Bluetooth v2.1 + EDR

Bluetooth Core Specification Version 2.1 + EDR is fully backward compatible with 1.2, and was adopted by the Bluetooth SIG on July 26, 2007.

The headline feature of 2.1 is secure simple pairing (SSP): this improves the pairing experience for Bluetooth devices, while increasing the use and strength of security. See the section on Pairing below for more details.

2.1 allows various other improvements, including "Extended inquiry response" (EIR), which provides more information during the inquiry procedure to allow better filtering of devices before connection; sniff subrating, which reduces the power consumption in low-power mode

Bluetooth v3.0 + HS

Version 3.0 + HS of the Bluetooth Core Specification was adopted by the Bluetooth SIG on April 21, 2009. It supports theoretical data transfer speeds of up to 24 Mbit/s, though not over the Bluetooth link itself. Instead, the Bluetooth link is used for negotiation and establishment, and the high data rate traffic is carried over a colocated 802.11 link. Its main new feature is AMP (Alternate MAC/PHY), the addition of 802.11 as a high speed transport. Two technologies had been anticipated for AMP: 802.11 and UWB, but UWB is missing from the specification.

Alternate MAC/PHY

> Enables the use of alternative MAC and PHYs for transporting Bluetooth profile data. The Bluetooth radio is still used for device discovery, initial connection and profile configuration, however when large quantities of data need to be sent, the high speed alternate MAC PHY 802.11 (typically associated with Wi-Fi) will be used to transport the data. This means that the proven low power connection models of Bluetooth are used when the system is idle, and the low power per bit radios are used when large quantities of data need to be sent.

Unicast connectionless data

> Permits service data to be sent without establishing an explicit L2CAP channel. It is intended for use by applications that require low latency between user action and reconnection/transmission of data. This is only appropriate for small amounts of data.

Enhanced Power Control

> Updates the power control feature to remove the open loop power control, and also to clarify ambiguities in power control introduced by the new modulation schemes added for EDR. Enhanced power control removes the ambiguities by specifying the behaviour that is expected. The feature also adds closed loop power control, meaning RSSI filtering can start as the response is received. Additionally, a "go straight to maximum power" request has been introduced, this is expected to deal with the headset link loss issue typically observed when a user puts their phone into a pocket on the opposite side to the headset.

Bluetooth v4.0

On June 12, 2007, Nokia and Bluetooth SIG had announced that Wibree will be a part of the Bluetooth specification, as an ultra-low power Bluetooth technology.

On December 17, 2009, the Bluetooth SIG adopted Bluetooth low energy technology as the hallmark feature of the version 4.0. The provisional names *Wibree* and *Bluetooth ULP* (Ultra Low Power) are abandoned.

On April 21, 2010, the Bluetooth SIG completed the Bluetooth Core Specification version 4.0, which includes *Classic Bluetooth*, *Bluetooth high speed* and *Bluetooth low energy* protocols. Bluetooth high speed is based on Wi-Fi, and Classic Bluetooth consists of legacy Bluetooth protocols.

Bluetooth low energy
Main article: Bluetooth low energy

Bluetooth low energy is an enhancement to the Bluetooth standard that was introduced in Bluetooth v4.0. It allows two types of implementation, dual-mode and single-mode. In a dual-mode implementation, Bluetooth low energy functionality is integrated into an existing Classic Bluetooth controller. The resulting architecture shares much of Classic Bluetooth's existing radio and functionality resulting in a minimal cost increase compared to Classic Bluetooth. Additionally, manufacturers can use current Classic Bluetooth (Bluetooth v2.1 + EDR or Bluetooth v3.0 + HS) chips with the new low energy stack, enhancing the development of Classic Bluetooth enabled devices with new capabilities.

Single-mode chips, which will enable highly integrated and compact devices, will feature a lightweight Link Layer providing ultra-low power idle mode operation, simple device discovery, and reliable point-to-multipoint data transfer with advanced power-save and secure encrypted connections at the lowest possible cost. The Link Layer in these controllers will enable Internet connected sensors to schedule Bluetooth low energy traffic between Bluetooth transmissions.

Expected use cases for Bluetooth low energy technology include sports and fitness, security and proximity and smart energy. Bluetooth low energy technology is designed for devices to have a battery life of up to one year such as those powered by coin-cell batteries. These types of devices include watches that will use Bluetooth low energy technology to display Caller ID information and sports sensors that will be used to monitor the wearer's heart rate during exercise. The Medical Devices Working Group of the Bluetooth SIG is also creating a medical devices profile and associated protocols to enable Bluetooth applications for this vertical market.

BLUETOOTH VOCABULARY

BlueBug	Issuing AT commands to place calls using another Bluetooth device
BlueDump	Watching Bluetooth pairing, using that info to crack a Bluetooth PIN
BlueJacking	Adding a new contact to a Bluetooth device's phonebook
BlueRogue	Using unauthorized Bluetooth devices, especially Access Points
BlueSmack	Sending an L2CAP ping-of-death to crash a Bluetooth device
BlueSnarfing	Grabbing contact and calendar lists from Bluetooth PDAs and phones device
BlueSniffing	Scanning an address range to find nearby Bluetooth devices
BlueSpoof	Masquerading as another Bluetooth device by using its BT address
BlueStab	Using bad names to crash devices engaged in Bluetooth discovery address
Bluetooone	Using external 2.4 GHz antenna to extend Bluetooth attack range
Cabir	Used Bluetooth to propagate a Symbian OS proof-of-concept worm

References

Wireless LAN

http://en.wikipedia.org/wiki/Frequency-division_multiplexing
http://en.wikipedia.org/wiki/Orthogonal_frequency-division_multiplexing
http://en.wikipedia.org/wiki/Frequency-hopping_spread_spectrum
http://en.wikipedia.org/wiki/Omnidirectional_antenna
http://en.wikipedia.org/wiki/Antenna_(radio)
http://en.wikipedia.org/wiki/Long-range_Wi-Fi
http://en.wikipedia.org/wiki/Wireless_LAN
http://en.wikipedia.org/wiki/IEEE_802.11n-2009
http://www.scribd.com/doc/13628928/80211-Protocol-Stack-and-Physical-Layer

Zigbee

http://en.wikipedia.org/wiki/File:Eazix_numbered.jpg
http://www.zigbees.com/
http://en.wikipedia.org/wiki/ZigBee
http://it.wikipedia.org/wiki/ZigBee http://zigbeeyoyo.blogspot.com/2007/08/zigbee.html
http://wiiifiii.igetweb.com/?mo=3&art=340802

Wimax

http://www.tutorial-reports.com/wireless/wimax/introduction.php
http://www.4gwirelessjobs.com/articles/article-detail.php?Ensuring-Security-in WiMAX&Arid=MTUx&Auid=NjM=
http://www.wimax.in.th/wimax/เทคโนโลยี-wimax/ http://en.wikipedia.org/wiki/WiMAX
http://www.wimax.com/general/what-is-wimax

Bluetooth

http://www.siamphone.com
http://www.computingunplugged.com/issues/issue200411/00001397001.html
http://www.bedd.com/
http://www.comms.scitech.susx.ac.uk/research/bluetooth.php
http://www.theregister.co.uk/2004/09/02/bluetooth_umbrella/
http://www.undertheumbrella.net/
http://www.cs.tcd.ie/courses/baict/bass/4ict9/Section2/Adhoc-Four2003.pdf
http://searchmobilecomputing.techtarget.com/resources/Bluetooth
http://www.wikipedia.org