ITS323 REPORT

Assignment 1

Prepared by

Pongsate Tangseng ID: 5122780786
Witchulada Saetang ID: 5122781503
Kapanai Vimolpatranon ID:5122791494

Submitted to

Dr. Steven Gordon

September 8, 2010

Table of Contents

1. Bluetooth

Protocol Architecture

Bluetooth is the device for wireless communication, data, and voice transmission especially in Personal Area Networks (PANs). The figure below shows the Bluetooth's protocol stack.

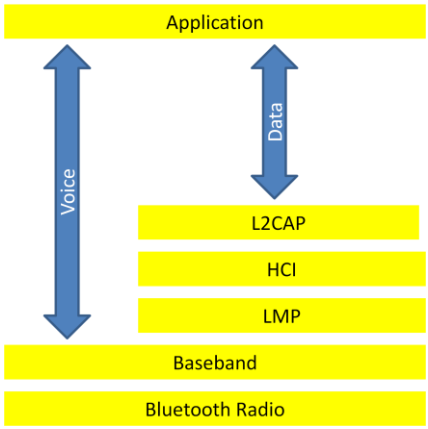


Figure 1.1 Bluetooth Protocol Stack

Bluetooth Radio Layer is the physical layer that tells about the specification of the transmission medium. Bluetooth operates in between 2.402 GHz and 2.480 GHz unlicensed ISM band (which is the same as WIFI) with 79 hop frequencies: f = 2402+k MHz, k= 0,..78. Bluetooth is able to share the same frequency band without experiencing any interference because it utilizes various key technologies such as frequency-hopping spread spectrum (FHSS).

Baseband Layer is responsible of controlling the transmission of packet though radio link and providing the channel for both data and voice.

Link Manager Protocol (LMP) use the link that setup by Baseband layer to connect to other device and also manage the security and monitoring service quality.

Host Controller Interface (HCI) is connection between hardware (LMP) and software (L2CAP).

Logical Link Control and Adaptation Protocol (L2CAP) connected to application layer and act as translator to translate the data from application to the Bluetooth format.

Bluetooth Standard

IEEE802.15 is the standard specification for Bluetooth. The Bluetooth Standard provides two types of links: synchronous connection-oriented (SCO) for voice exchange and asynchronous connectionless (ACL) links for data packets. All types of packets except AUX1 are protected by cyclic redundancy check (CRC) and automatic repeat request (ARQ) scheme for error control. Moreover, in order to mitigate the fading effects and other packet loss sources, three times repetition for forward error correction (FEC) is applied in the header and the payload of the data medium rate (DM) packets is protected by shortened Hamming code for FEC with rate of 2/3. However, no such coding is applied by data high rate (DH) packets and the error probabilities of transmitted data are higher. Then it will be worth comparing system's performance when DM and DH packets are exchanged.

Nowadays, 4 standards of Bluetooth are announced: Bluetooth 1.0, Bluetooth 1.1, Bluetooth 1.2, and Bluetooth 2.0 with 2 additional Enhance Data Rate (EDR) versions, Bluetooth 2.0 EDR and Bluetooth 2.1 EDR.

Bluetooth's Network System

Bluetooth is packet-based protocol with a master slave structure. The network is called piconet. A piconet can consist of 1 master and up to 7 active slaves with up to 255 inactive slaves.

Data Transmission:

Frequency

Operates in the 2.45 gigahertz (actually between 2.402 GHz and 2.480 GHz, to be exact) unlicensed ISM band. ISM band is specific range of radio band that reserved for industrial, scientific and medical purpose only.

Bluetooth is able to share the same frequency band without experiencing any interference because it utilizes various key technologies.

79 hop frequencies: f = 2402+k MHz, k= 0,..78.

Gaussian Frequency-Shift Keying (GFSK) modulation: BT=0.5, 0.28 < m < 0.35.

Spectrum

Bluetooth uses a technique called frequency-hopping spread spectrum (FHSS)**.** FHSS is a method that used to solve a problem about narrowband interference by rapidly switch carrier among many frequency channels in a specific sequence that both transmitter and receiver know. In case of Bluetooth the transmitters change frequencies 1,600 times every second. FHSS made Bluetooth radio signal also hard to intercept because the frequency of carrier is changed rapidly, as a result, the privacy of the data that is transmitted increased.

Data rate

Configuration	Max. Data Rate Upstream	Max. Data Rate Downstream
3 Simultaneous Voice Channels	64 kb/sec X 3 channels	64 kb/sec X 3 channels
Symmetric Data	433.9 kb/sec	433.9 kb/sec
Asymmetric Data	723.2 kb/sec or 57.6 kb/sec	57.6 kb/sec or 723.2 kb/sec

Table 1.2 Bluetooth Data rate

Transmission Media

Power Class	Maximum Output Power (Pmax)	Minimum Output Power (Pmin)	Distance (Meter)
1	100 mW (20 dBm)	1 mW (0 dBm)	100
2	2.5 mW (4 dBm)	0.25 mW (-6 dBm)	10
3	1 mW (0 dBm)	N/A	1

Table 1.3 Bluetooth Transmitting power and distance

From the table above, the transmit power of Bluetooth is divided into 3 classes; 100mW, 2.5mW, 1mW for class 1, 2, and 3 respectively.

Receiver Sensitivity

Block Error Rate (BER) 0.1% for sensitivity of –70dBm input power level, 11 dB carrier to co-channel interference ratio.

Bluetooth Packet

Bluetooth packet has 2 versions according to Bluetooth standard: Basic Rate packet and Enhance Data Rate (EDR) packet.

The general Basic Rate packet consists of 3 entities: the access code, the header, and the payload.

The general Enhanced Data Rate packet consists of 6 entities: the access code, the header, the guard period, the synchronization sequence, the Enhanced Data Rate payload and the trailer.

Signal Encoding Technique

Bluetooth use Gaussian Frequency Shift Keying (GFSK) for encoding digital data into analog signal with a bandwidth bit period product BT=0.5.

In EDR version, the payload part and trailer part of Bluetooth packet will be encoded and decoded using Phase Shift Keying (PSK) scheme with addition of guard bits to separate between the part that has to be decoded with GFSK and the part that has to be decoded with PSK.

Error Correction

Automatic Repeat Request unnumbered scheme (ARQ) is provided in baseband layer. Bluetooth also use 1/3 and 2/3 rate Forward Error Control (FEC).

Application

- Wireless connection between a mobile phone and a hand-free headset.
- Wireless networking between PCs.
- Wireless communication with PC input and output devices.
- Data and information transfer between handheld devices and between handheld devices and PC.
- Replacement of traditional wired serial communications in test equipment, GPS receivers, medical equipment, bar code scanners, and traffic control devices.
- Use Bluetooth instead of infrared.
- For application that use low bandwidth and require wireless.
- Wireless controller for game consoles, Nintendo's Wii and Sony's PlayStation 3 and PSP Go.
- Short range transmission of health sensor data from medical devices to other handheld devices
- Allowing a Digital Enhanced Cordless Telecommunications (DECT) phone to ring and answer calls on behalf of a nearby cell phone

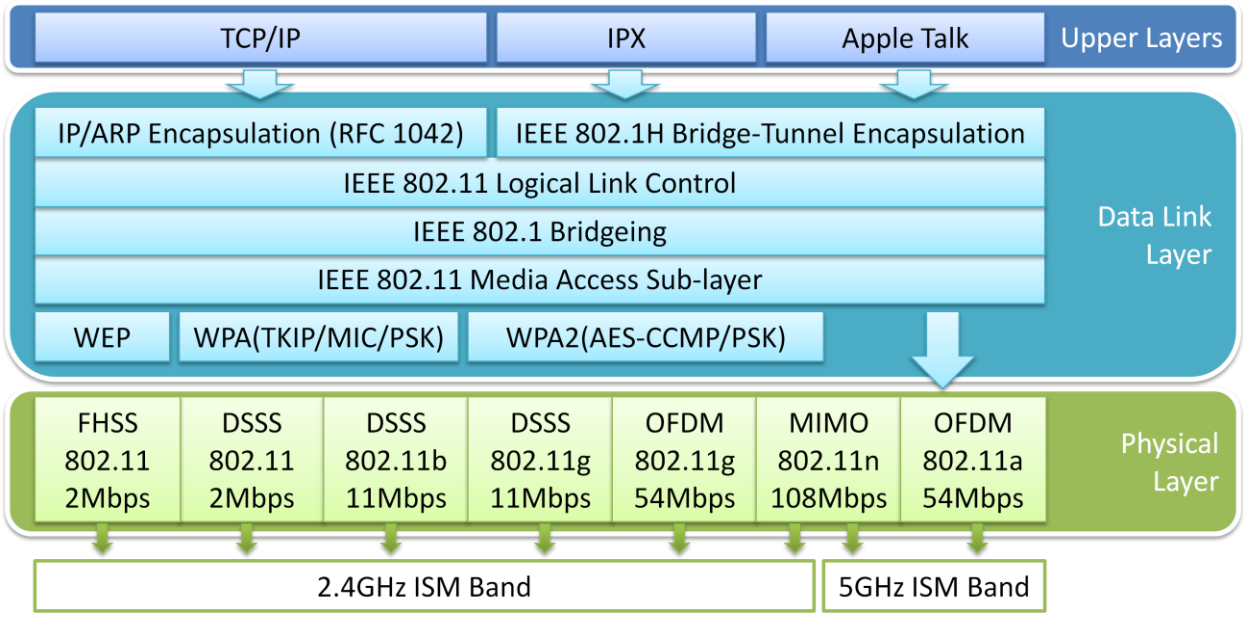
Cost

The cost of Bluetooth is essentially only the cost of Bluetooth chip which is around $4. The cost of communication is free because Bluetooth's radio spectrum is unlicensed. The cost that costumer actually pay is the cost of device that Bluetooth is installed.

Since the cost of Bluetooth is quite low, easy to use, and embedded in almost wireless device, Bluetooth become popular in the world of wireless communication and used around the world.

2. Wireless Local Area Network (WLAN)

Protocol Architecture



The WLAN is in the family of IEEE 802.11 protocol standard. IEEE 802.11 specifications cover on Physical layer and Media Access (MAC) Layer. In Physical layer part, IEEE 802.11 defines that the equipment must have data rate at 1, 2, 5.5, 11 and 54 Mbps. In MAC layer part, IEEE 802.11 defines that the equipment must use Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA) for path sharing. In addition, IEEE 802.11 also defines that the equipment must have the encryption and authentication method named Wired Equivalent Privacy (WEP).

There are four specifications in IEEE 802.11 family. Table below shows the detail of each specification.

Specification	Data rate (Mbps)	Frequency (GHz)
IEEE 802.11	1-2	2.4
IEEE 802.11a	6,12,24,54	5
IEEE 802.11b	1-11	2.4
IEEE 802.11g	20-54	2.4
IEEE 802.11n	100-200	2.4

Table 2.1 WLAN Standard and Frequency used.

Data rate (Mbps)	Minimum Sensitivity (dBm)	IEEE802.11a OFDM	IEEE802.11b DSSS	IEEE802.11g DSSS and OFDM
1			Barker(BPSK)	Barker(BPSK)
2			Barker(QPSK)	Barker(QPSK)
5.5			CCK(QPSK)	CCK(QPSK)
6	-82	OFDM(BPSK)		OFDM(BPSK)
9	-81	OFDM(BPSK)		OFDM(BPSK)
11			CCK(QPSK)	CCK(QPSK)
12	-79	OFDM(QPSK)		OFDM(QPSK)
18	-77	OFDM(QPSK)		OFDM(QPSK)
24	-74	OFDM(16QAM)		OFDM(16QAM)
36	-70	OFDM(16QAM)		OFDM(16QAM)
48	-66	OFDM(64QAM)		OFDM(16QAM)
54	-65	OFDM(64QAM)		OFDM(64QAM)

Table 2.2 IEEE Standard and Modulation used for difference data rate

Narrowband

Narrowband is technique that used the narrow radio frequency in range 902 MHz to 928 MHz, 2.14 MHz to 2.484, and 5.725 MHz to 5.850 MHz. The power of this signal is quite low (approximately 1mW) and used with 1 pair of transmitter-receiver only.

Spread Spectrum

Spread Spectrum is technique that widely used in wireless network system. This technique used frequency in range between 902-928 MHz to 2.4-2.484 GHz. This technique can be divided into 2 patterns: Frequency hopping spread spectrum (FHSS) or direct sequence spread spectrum (DSSS).

Frequency hopping spread spectrum (FHSS)

In IEEE 802.11 and IEEE 802.11n standard, WLAN may use a technique called frequency-hopping spread spectrum (FHSS). FHSS is a method that used to solve a problem about narrowband interference by rapidly switch carrier among many frequency channels in a specific sequence that both transmitter and receiver know. The IEEE 802.11 standard provides 22 hop patterns, or frequency shifts, to choose from in the 2.4-GHz ISM band. FHSS made WLAN radio signal also hard to intercept because the frequency of carrier is changed rapidly, as a result, the privacy of the data that is transmitted increased.

Direct sequence spread spectrum (DSSS)

In IEEE 802.11 and IEEE 802.11n standard, WLAN may use a technique called direct sequence spread spectrum (DSSS) too. DSSS break down the chunk of data into small pieces and send across frequency channel. A redundant bit pattern (known as a chipping code) is generated for each bit transmitted to check whether the data is transmitted correctly or not. DSSS use more bandwidth than FHSS but it is considered more reliable and resists interference because the use of a chipping code.

Barker code

Barker code is the sequence of value that used in DSSS only in IEEE802.11b standard at 1-2 Mbps of data rate. This makes for a more uniform spectrum, and better performance in the receivers.

Complementary code keying (CCK)

Complementary Code Keying (CCK) is the complementary codes are a set of nearly orthogonal complex sequences that was adopt to be the supplement of Barker Code to achieve higher data rate with shorter distance. CCK has higher data rate than Barker Code because it has more chipping sequences (4 chipping sequences at 5.5 Mbps and 64 chipping sequences at 11 Mbps compare to single chipping sequence). CCK is used in IEEE082.11b.

Orthogonal frequency division multiplexing (OFDM)

In IEEE 802.11a and IEEE 802.11g standard which give higher data rate (54 Mbps), WLAN use a technique called orthogonal frequency division multiplexing (OFDM). OFDM is the variation of multi-carrier transmission that able to send many pieces of data at the same time via many frequency of carrier signal. The additional feature of OFDM over a regular multi-carrier transmission is every subcarrier is orthogonal to each other. As a result, data rate is increased.

Transmission Media

Range

WLAN Standards do not specify the range of transmitting because the range is greatly depending on many factors. Range and data rate of WLAN greatly depend on the obstacles between transmitter and receiver. Table below shows the relationship between some obstacle and the power of signal. The range (or radius of coverage) for typical WLAN systems varies from under 100 feet to more than 500 feet.

Obstacles	2.4 GHz	5 GHz
Concrete 18”	18dB	30dB
Brick 3.5”	6dB	10dB
Drywall	3dB	5dB
Free Space 10 m.	60dB	68dB
Free Space 100 m.	80dB	88dB

Table 2.3 Signal Attenuation

Antennas

Antenna for IEEE802.11 has 2 types: directional and omnidirectional. Most device use omnidirectional version.

WLAN Network Topology

WLAN can be separate into 2 categories:

1. Peer to Peer (Ad-hoc)

Ad-hoc network is the closed network of data communication between 2 or more device without central control node. Closed network means there is no host node and no communication with other network. Every device can communicate with each other because the device transmits signal in every direction without knowledge of receiver's location. The receivers need to intercept every frame that in the receiver's range and check that the frame is actually target at the receiver or not by looking at MAC address.

2. Infrastructure (Client/Server)

Normally, devices in IEEE802.11 WLAN are connected in infrastructure mode. In this mode, there are 2 types of devices; Client Station and Access Point. Client Station is an ordinary electric device (PC, Cell Phone, Laptop, and etc.) that install client adapter for transfer date in IEEE802.11 standard. Access Point is a special device that connects the network with other network (usually IEEE802.3 Ethernet LAN). Every client must connect to the Access Point only. The Access Point will forward the data from client to the destination or receive data from other source and send to client.

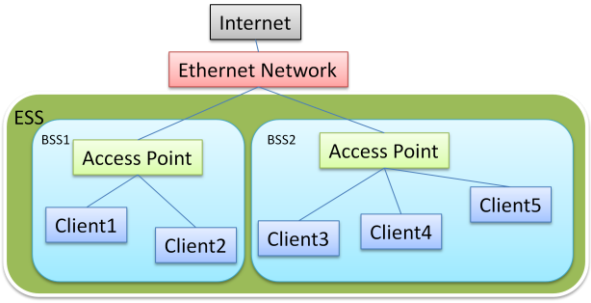


Figure 2.4 ESS and BSS

Basic Service Set (BSS)

Basic Service Set (BSS) is region of IEEE802.11 WLAN network that has only 1 access point. Every client in this BSS must communication with access point in the region only.

Extended Service Set (ESS)

Extended Service Set is the region of IEEE802.11 WLAN network that contain more than 1 BSS that connected together. The access point can move from a BSS to another BSS then every BSS will roaming for changing service for every client in the BSS.

Channel Management

Duty of MAC Layer in IEEE802.11 standard is channel management. Each BSS must share channels effectively. IEEE 802.11 defines that the equipment must use Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA) to manage channels.

Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA)

CSMA/CA is channel management technique. The principle of CSMA/CA is when a station wants to use a channel; the station has to verify that the channel is being used by other station or not by sending data and wait for acknowledgement respond. If no respond in a period of time then the station know that the channel is being used. The station has to send the data again.

Signal Encoding Technique

Phase-Shift Keying (PSK)

In order to transmit digital data over WLAN, digital data need to be encoded into analog signal using 2 variations of Phase-Shift Keying (PSK), Binary Phase-Shift Keying (BPSK), Quadrature Phase-Shift Keying (QBSK) and Quadrature amplitude modulation.

Quadrature amplitude modulation (QAM)

QAM is one the many derivations of Amplitude Modulation. QAM convert the digital data to analog signal by change the amplitude of two waves, 90 degrees out-of-phase with each other (in quadrature). Amplitude modulating two carriers in quadrature can be equivalently viewed as both amplitude modulating and phase modulating a single carrier.

16 state Quadrature amplitude modulation (16-QAM)

16-QAM is derivation of QAM that use 4 carrier phases and 4 carrier amplitudes. So, in one wave, 4 bits of data can be sent.

Symbol Transmitted	Carrier Phase	Carrier Amplitude
0000	225°	0.33
0001	255°	0.75
0010	195°	0.75
0011	225°	1.0
0100	135°	0.33
0101	105°	0.75
0110	165°	0.75
0111	135°	1.0
1000	315°	0.33
1001	285°	0.75
1010	345°	0.75
1011	315°	1.0
1100	45°	0.33
1101	75°	0.75
1110	15°	0.75
1111	45°	1.0

Table 2.3 16-QAM

64 state Quadrature amplitude modulation (64-QAM)

64-QAM is derivation of QAM that use 8 carrier phases and 8 carrier amplitudes. So, in one wave, 8 bits of data can be sent.

Error control

WLAN may have high error rates due to attenuation, fading, or interfering active radiation sources. WLAN used Forward Error Control (FEC) to detect and correct errors that occur in the transmission.

Application

WLAN is suitable for install on the place that cannot have the cable. Also useful when there are many equipment that need to access the network at the same time because it's wireless then it's no need to have any wires or place to plug the line in. WLAN also for transfer the big size of data because the data rate of WLAN is quite high (usually 54 Mbps).

The concrete example of WLAN usage is to be the supplement of typical wired LAN that use coaxial cable.

WLAN can be embedded in handheld devices such as mobile phone, PDA, Sony PSP and Nintendo DS for fast wireless communication or internet surfing.

But there is a down side of the high data rate of WLAN. Since the data rate is high and the device is quite complicate, so it's not suitable for very long-time operation but low data transmission such as fire alarm for remote controller.

Cost

A cost of WLAN is the cost of the wireless access points for infrastructure for and the wireless LAN adapters for user. The cost of access point is approximately between $800.00 and $2,000.00 per each. The number of access points depends on the size of the require area and the number of client.

Clients need a WLAN adapters per an equipment (PC, cell phone, PDA, etc.). The cost of WLAN adapter is range from $200.00 to $700.00. Maintenance cost is low compare to wired LAN because there is no wired to maintain, and the modification can be done easily without moving wire.

3. WiMax

WiMax standard

IEEE 802.16 Standards

WiMax Standard Differences

This figure shows a comparison between the original Fixed WiMax standard and the WiMax standard that can be used for fixed, mobile and portable.

Characteristic	Fixed WiMax	Mobile WiMax
Industry Standard	802.16 (2004)	802.16e (2005)
Access Type	Fixed	Fixed, Portable and Mobile
Modulation	OFDM	OFDMA
Duplexing	TDD,FDD	TDD,FDD Optional
Handoffs	No	Yes
Types of Service Providers	DSL, Cable Modems and Competitive Access Provider (CAPs)	Mobile Operators, DSL, Cable Modems, Wireless and Wired ISPs
Subscriber Units	High Performance Outdoor and Indoor CPE	Low Cost Consumer Electronics CPE and Embedded Modules
Preferred Frequency Bands	2.5 GHz, 3.4-36 GHz, 5.8 GHz	2.3-2.4 GHz, 2.5-2.7 GHz, 3.3-3.4 GHz, 3.4-3.8 GHz

Table 3.1 WiMax Specification

Stack Layer

WiMax divided layer into Physical layer (PHY-Layer) and Medium access control layer (MAC-Layer).

Physical Layer

Physical layer can be used to Encoding/decoding of signals, Preamble generation/removal and Bit transmission/reception

Data Link layer (MAC Layer)

The IEEE 802.16 MAC was designed for point-to-multipoint broadband wireless access applications. The primary task of the WiMax MAC layer is to provide an interface between the higher transport layers and the physical layer.

On transmission,

Collect data into a frame with address and error detection fields

On reception,

Take a part of frame, and perform address recognition and error detection access to the wireless transmission medium.

Channel Bandwidth	3.5 MHz		1.25 MHz		5 MHz		10 MHz	
PHY mode	256 OFDM		128 OFDMA		512 OFDMA		1,024 OFDMA	
Oversampling	8/7		28/25		28/25		28/25	
Modulation & Code Rate	PHY-Layer Data Rate (kbps)							
	DL	UL	DL	UL	DL	UL	DL	UL
BPSK, 1/2	946	326	NOT APPLICABLE					
QPSK, 1/2	1,882	653	504	154	2,520	653	5,040	1,344
QPSK, 3/4	2,822	979	756	230	3,780	979	7,560	2,016
16 QAM, 1/2	3,763	1,306	1,008	307	5,040	1,306	10,080	2,688
16 QAM, 3/4	5,645	1,958	1,512	461	7,560	1,958	15,120	4,032
64 QAM, 1/2	5,645	1,958	1,512	461	7,560	1,958	15,120	4,032
64 QAM, 2/3	7,526	2,611	2,016	614	10,080	2,611	20,160	5,376
64 QAM, 3/4	8,467	2,938	2,268	691	11,340	2,938	22,680	6,048
64 QAM, 5/6	9,408	3,264	2,520	768	12,600	3,264	25,200	6,720

Table 3.2 shown different modulation and channel details

Antenna

WiMax has a long transmission range up to 31 miles because regulations allow WiMax systems to transmit

2 types of antennas

Unidirectional Antennas and Omni-Directional Antennas

Frequency

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. 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**.** Ex. Canada use 2.3, 2.5, 3.5, 5.8 GHz, and USA use 2.3, 2.5, 5.8 GHz

Bandwidth

As you see from Table 3.2:3.5, 1.25,5,10 MHz

Signal Encoding Techniques

As Table 3.2

OFDM and OFDMA: The Difference

IEEE 802.16d (fixed service) uses Orthogonal Frequency Division Multiplexing (OFDM).

IEEE 802.16e (mobile) uses Orthogonal Frequency Division Multiple Access (OFDMA).

We have used OFDM for a while in some technology such as ADSL. WiMax is the technology that uses S-OFDMA (Scalable- Orthogonal Frequency Division Multiple Access). With the high efficiency underneath its bandwidth make the WiMax have a very high data rate.

What's OFDM?

OFDM is Orthogonal Frequency Division Multiplex. Main major is Multiplex the multiple channels or separate the channel with frequency. Therefore, they try to increase the efficiency of Multiplexing on frequency, which is Orthogonal.

Orthogonal is the ways that make the channels independently to each other and can't have impacts to each other. If we can manage the frequency in each channel to be orthogonal to each other, there's no necessity to have Guard band for protected the disturbance of each other. So the frequency will be more efficient.

From OFDM to OFDMA

OFDMA is the way to separate the channel (Subcarrier) to each user. But the way of separation is combining between TDMA and FDMA which is change of frequency channel from time to time. The number of channel will be depending on the quantity of the services.

The advantage of separation is it will help spread the risk that come from the disturbing signal especially Narrow band interference. If there's any disturbing signal, the signal that missing will be just a component and temporarily. So we can fix with using Error Coding so the quantity of signal will be better.

For WiMax, WiMax use the technology S-OFDMA (Scalable OFDMA) which the difference is the number of subcarriers that use with the user can be able to modify because of using 802.16e will have movement that hand off between the station and might cause the changed of numbers of channel.

Transmit power

WiMax Base Station (Fix) has the transmit power at +43 dBm (20 W) and Mobile Station has the transmit power at +23 dBm (200 mW).

Receive thresholds

WiMax Base Station (Fix) has the receive thresholds Up to 5 dB SNR and Mobile Station has the receive thresholds Up to 10.5 dB SNR

Distance

Max distance of WiMax Base Station: Fix is 75km and Mobile Station is 2-4 km.

Error Detection Techniques in WiMax Technology

WiMax use Hybrid automatic repeat request (Hybrid ARQ or HARQ)

How's WiMax in Thailand?

In the first era *Broadband* Wireless Access technology is used to emphasize on the Point-to-Point connection which is the connection of network between two buildings for the communication. Later on, the connection has many conditions and limited so there's a new development of the new connection technology call Point-to-Multipoint. With this technique, broadband service can cover more area than it used to be. So in the business it's worth it for the investment.

Therefore, Broadband wireless access technology is the technology that help the service can expand the area to make a broadband service quickly and efficient. Moreover, the budget of the investment is low.

There's the continuously growth of Broadband around the world especially in Asia in this few years. And it is still continuously growth because of the demand of high speed communication.

Cost

WiMax cost is relative low compare to broadband DSL and 3G. Broadband DSL is wired which very expensive both in investment and maintenance. 3G is packet-based and the service charge is depending on the amount of data that has been transferred which is very expensive if users need to transfer a lot of data. The cost of WiMax adapter is around $20 - $299.

Advantages

1. Coverage for hundred of users at a time and manage sending and receiving of data at very high speed with full of network security.
2. WiMax Technology performs many tasks at a time.
3. WiMax provides a low cost network.
4. WiMax offers separate voice and data channel, the semantic connection make your network more secure than before, fast connectively, license spectrum, liberty of movement and more.
5. Antenna in WiMax network offering high quality widest array which so you can communication on long route without any encryption.

Disadvantages

1. The **major disadvantage of WiMax** is its installation and operational cost. Because of its heavy structure, tower, antennas etc makes the WiMax network is a high cost network.
2. WiMax need much electrical support for running the overall network.
3. The data rate of WiMax is very slow compared to other network such as fiber optics, satellite.

4. ZigBee

Characteristics of ZigBee

- **Band** – 868, 902-928MHz, and 2.4GHz
- **Topology** – Ad-hoc, Star, Point to Point, Mesh
- **Data Rate** – 20/40Kb/s and 250Kb/s
- **Power Consumption** – Very Low
- **Range** – 10-100+ meters
- **Security** – very high; AES-128 level encryption
- **Size** – up to 64K nodes in a single logical network

ZigBee protocol

The network of ZigBee protocol has 3 control equipments

1. Coordinator
2. End device
3. Router

Coordinator

Use FFD for IEE Device type and it typical function are one per network, Forms the network, allocates network address and holds binding table.

Router

Use FFD for IEE Device type, and it typical function are extends the physical range of the network, Allows more nodes to join the network and my also perform monitoring and/or control functions.

End device

Use FFD or RFD IEE Device type, and it typical function is to perform monitoring and control functions.

ZigBee layers

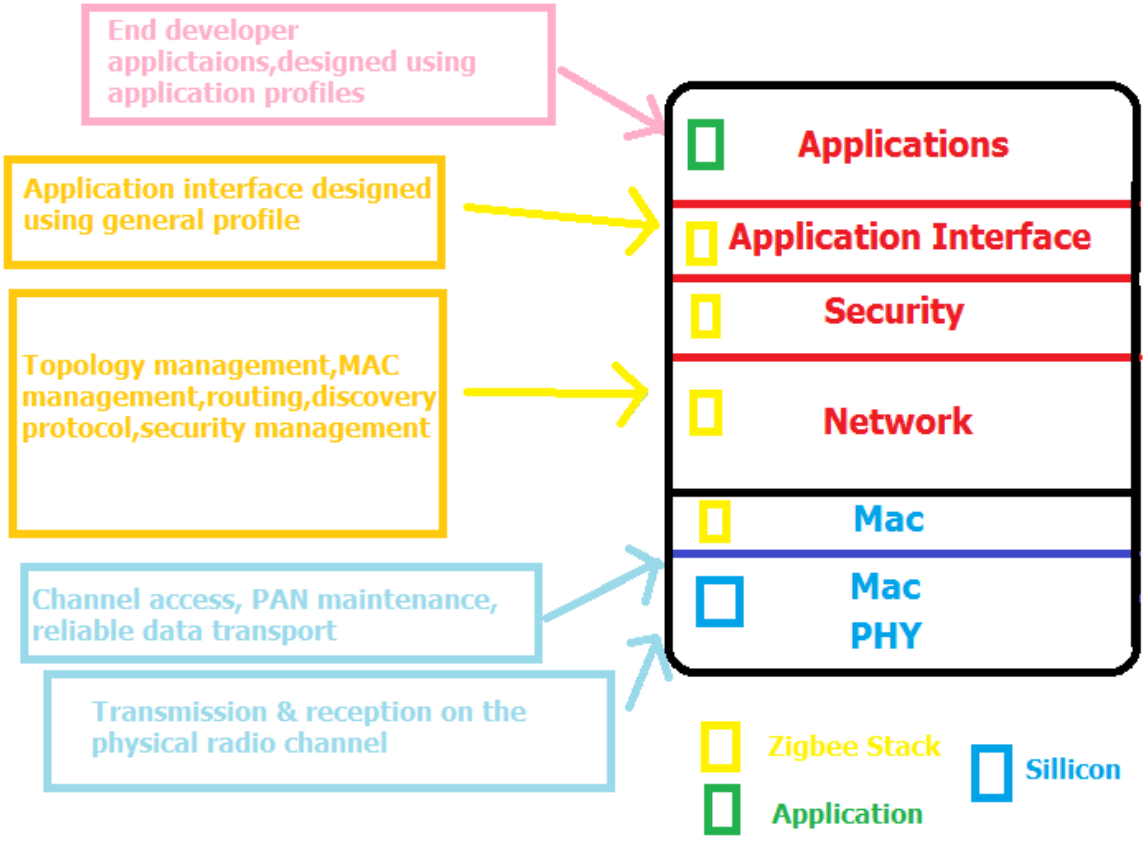


Figure 4.1 ZigBee protocol layers

The ZigBee stack is loosely based on the OSI 7-layer model. It implements only the functionality that is required in the intended markets.

Physical layer

The physical layer consists of RF Transceiver and Low Level Control Mechanism

The physical layer is used to activation or deactivation of the radio transceiver, Energy Detection , Link Quality Indication , channel selection , Clear Channel Assessment and receive packets through the mediums.

Physical layer has 2 kinds which is data service and management service. Physical later can be used to turn on and off radio-transceiver, Energy Detection, Link Quality Indication, channel selection, Clear Channel Assessment and send or receive the packet

In 2.4 GHz to 2.4835 GHz frequency has 16 channels in communicating (figured 4.2)

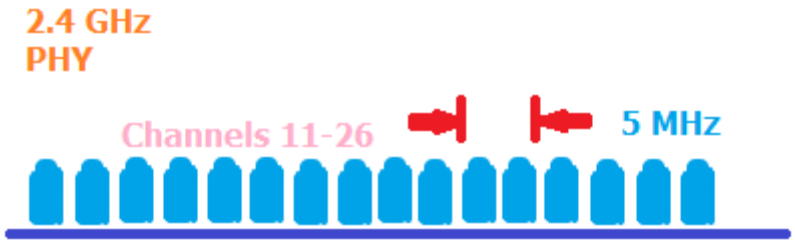


Figure 4.2 ZigBee frequency channels

MAC layer

MAC layer is designed for using topology with many types and not complicated so we can use it with many kind of instrument and MAC layer also help Physical Channel.

Network layer

Network layer is use to search for the route (routing) from source to destination that might be in the same or different network. The main function of this layer is to correct use of the MAC sub layer and provide a suitable interface. It structure are associated to such network layers. The function of network layer has ability to starting a network by having a ability to successfully create a new network. Ability to gain membership or relieve membership a network also routing, and security such as applying security to outgoing frames and removing security to terminating frames.

Comparison of ZigBee Devices at the Network Layer

ZigBee Network layer function	Coordination	Router	End Device
Establish a ZigBee network	/		
Permit other devices to join or leave the network	/	/	
Assign 16-bit network addresses	/	/	
Discover and record paths for efficient message delivery	/	/	
Discover and record list of one-hop neighbors	/	/	
Route network packets	/	/	
Receive or send network packets	/	/	/
Join or leave the network	/	/	/
Enter sleep mode			/

Table 4.3 Comparison of ZigBee devices

Application layer

The application layer is the highest-level layer defined by the specification, and is the effective interface of the ZigBee system to its end users. Application layer is a layer that has endpoint call “application framework” ZigBee device object used to reach and use the application layer.

Application support sub-layer

Application support sub-layer is used to build the frame of application layer and have the function of sending and receiving the data included management procedure, together with application objects defined by the manufacturer, are considered part of this layer.

The APS sub-layer is responsible for:

- binding tables
- message forwarding between bound devices
- group address definition and management
- address mapping from 64-bit extended addresses to 16-bit NWK addresses
- fragmentation and reassembly of packets
- reliable data transport

ZigBee Standard

ZigBee use IEEE standard 802.15.4(2003 version) which is for low-rate WPAN's. This standard low rate of communication, low power supply needed, cheap instrument and has the performance to manage itself. The specific will complete the standard by adding four main components: network layer, application layer, ZigBee device objects (ZDO's)

ZDO is a specialized application object called the ZigBee Device Object. It is addressed as endpoint 0.

ZigBee also manufacturer-defined application objects which allow for customizing total composition and favor composition. The most important improvement is ZDO's. There are responsible for many tasks such as keeping of device roles, management of requests to join a network, device discovery and also security.

ZigBee Frequency

ZigBee is targeted at radio-frequency (range of about 30 kHz to 300 GHz) applications that require a low data rate, long battery life, and secure

For Standard IEEE 802.15.4 in Physical layer has 3 range of frequency which is 2.4-2.4835 GHz bit rate 250 kb/s have 16 channels from channel 11 to 26 , 868-870 MHz bit rate 20 kb/s have 1 channel in channel 0 , 902 - 928 MHz bit rate 40 kb/s have 10 channel from channel 1 to 10

In 2.4-2.4835 GHz, frequency can use in every area in the world and frequency 868-870 MHz and 902-928 MHz can use in North America area , Europe , Australia and New Zealand

Fc = 2405 + 5(k-11) (1) for k = 11, 12, …, 26 where k=number of channel.

ZigBee Transmission range

Transmission range is between 10 and 75 meters (33 and 246 feet) and for ZigBee pro the range up to 1500 meters, although it is heavily dependent on the environment. The maximum output power of the radios is generally 0 dBm (1 mW).

Transmission power

The transmit power is consistent within 1dB. The minimum amount of energy needed to transmit output power of –3 dBm with a nominal 0 dBm output power.

Antenna

The gain of the antenna ranges from –5 to +2 dBi depending on the polar angle. The gain excludes the nulls. The nominal gain of the antenna is 0 dBi.

Data rate

The data rate for ZigBee technology is 250kbps (peak information rate 128kbps) compared to 720kbps for Bluetooth wireless technology. Transmitting at a higher data rate allows the system to shut down the transmitter and receiver more quickly, saving significant power. Higher data rates at a given power level mean there is less energy per transmitted bit, which reduced the range.

Error

ZigBee use error detection by using cyclic redundancy and repeat transmissions for reliable communication, but no error correction. The error control that suitable for ZigBee is hybrid-ARQ

Hybrid – ARQ is used to reduce the number of transmissions, we add redundancy in each transmission.

Signal Encoding Technique

ZigBee devices use 2 schemes Offset-quadrature-phase-shift keying (OQPSK) and DSSS (Direct Sequence Spread Spectrum) for modulating radio-signals in physical layer.

Offset-QPSK

Offset Quadrature Phase Shift Keying (Offset-QPSK) is a digital modulation scheme that carries data by changing, or modulating, the phase of a reference signal

Application of ZigBee

Applications of ZigBee have divided into 3 types by the type of information

1. *Periodic information* is information that can control the data rate, detect the stimulate signal, check the information and make the information stable Ex. Sensor and miter
2. *Intermittent information* can transmit the data when used. Ex. Light switch
3. *Repetitive low latency* use when we need very few latency the communication will apportion the time slot and also can use GTS mechanism for assure the quantity of the service Ex. Wireless mouse

Topology of ZigBee

Star Networks (Personal Area Network)

- Home automation
- PC Peripherals
- Personal Health Care

Peer-to-Peer (ad hoc, self organizing & healing)

- Industrial control and monitoring
- Wireless Sensor Networks
- Intelligent Agriculture

Cost of ZigBee

Cost of ZigBee transceiver is around $1 and one radio, processor, memory package is about $3.

5. Comparison

	ZigBee	Bluetooth	WLAN	WiMax
Standard	IEEE802.15.4	IEEE802.15.1	IEEE802.11	IEEE802.16
Bandwidth	250kbps	1Mbps	Up to 54Mbps	Maximum bandwidth of 70 Mbps
Stronghold	Long Battery Life, Low cost	Interoperability, cable replacement	High data rate	Communication on long route without any encryption
Application	Remote control, battery-operated product, sensors	Wireless USB, handset, headset, telecom audio, cable replacement	Internet browsing, PC networking, file transfers, enterprise and home access point	Quadruple Play services, VoIP, IPTV and Internet access
Network topology	Mesh networking	Star topology	Star topology	Star topology
Frequency	2.4-2.4835 GHz, 868-870 MHz, 902 - 928 MHz	2.45 GHz	2.4, 5 GHz	Up to 6.6 GHz

Table 5.1 Wireless communication technologies comparison

Protocol Architecture

WLAN standard is IEEE 802.11 family which define MAC layer to use CSMA/CA for channel management and has to use WEP for the encryption and authentication.

Bluetooth standard is IEEE 802.15.1 family which provides 2 types of link separated by type of data (voice and data) which use difference connection technique (SCO and ACL).

ZigBee standard is IEEE 802.15.4 family which is for low-rate WPAN's. This standard is especially for low rate of communication, low power supply needed, cheap instrument and has the performance to manage itself.

WiMax standard is IEEE 802.16 which is capable to penetrate the obstacle.

Data Transmission

WLAN's has 2 group of frequency: around 2.4 GHz and 5 GHz depend on the standard. WLAN use many kind of frequency modulation such as FHSS, DSSS, Barker Code, CCK and OFDM depend on data rate and standard. Data rate of WLAN is vary from 1mbps to 54 mbps depend on standard of WLAN.

Bluetooth's frequency is around 2.4 GHz as WLAN. Bluetooth has received threshold at -70 dBm. Bluetooth use FHSS for frequency modulation. Data rate of Bluetooth is up to 723 kbps for asymmetric data.

ZigBee's frequency is around 2.4 GHz as WLAN and Bluetooth. ZigBee use DSSS for frequency modulation. Data rate of ZigBee is up to 250 kbps which is also lowest.

WiMax's frequency is up to 6.6 GHz depend on type (Fixed, Mobile). WiMax Base Station (Fix) has the receive thresholds Up to 5 dB SNR and Mobile Station has the receive thresholds Up to 10.5 dB SNR. WiMax use OFDM and OFDMA for frequency modulation. Data rate of WiMax is up to 70 mbps which is highest in 4 technologies.

Transmission Media

WiMax has the most transmission power at 20W (Base station) and the longest transmitting range at 75 km.

WiMax has the least transmission power at 1mW and the shortest transmitting range at 75 m.

WLAN has lowest received threshold at -82 dBm which has data rate equal to 6 mbps.

Bluetooth has received threshold at -70 dBm.

ZigBee has received threshold at -92 dBm which is lowest of 4 wireless communication technologies.

WiMax Base Station (Fix) has the receive thresholds Up to 5 dB and Mobile Station has the receive thresholds Up to 10.5 dB.

Signal Encoding Technique

WLAN use BPSK, QPSK, 16-QAM and 64-QAM for encoding digital data to analog signal.

Bluetooth use GFSK for encoding digital data into analog signal with a bandwidth bit period product BT=0.5 and PSK in EDR version.

WiMax use BPSK, QPSK, 16-QAM and 64-QAM as same as WLAN.

Zigbee use Offset-QPSK.

Error

- Bluetooth use Automatic Repeat Request unnumbered scheme (ARQ) for error correction and also use 1/3 and 2/3 rate Forward Error Control (FEC).
- WLAN used Forward Error Control (FEC) to detect and correct errors that occur in the transmission.
- WiMax use Hybrid automatic repeat request (Hybrid ARQ or HARQ)
- ZigBee use error detection by using cyclic redundancy and repeat transmissions for reliable communication, but no error correction. The error control that suitable for ZigBee is hybrid-ARQ

Application

- WLAN can be embedded in handheld devices such as mobile phone, PDA, Sony PSP and Nintendo DS for fast wireless communication or internet surfing.
- For ZigBee the example of applications are Remote control, battery-operated product, sensors

- For WLAN the example of applications are Internet browsing, PC networking, file transfers, enterprise and home access point
- Applications of WiMax are Quadruple Play services, VoIP, IPTV and Internet access

In a fixed environment, such as the home, WiMax makes high-speed access a reality. WiMax is suitable for the area that no other signal can be reach. WiMax signal is more powerful than others because the WIMAX signal can pass though the rough terrain and also longer distance than the others.

The range of wireless LAN is not very far. It can be used in the small place such as house, office, school etc.

ZigBee is suitable only in the small area. ZigBee can be used as Remote control, battery-operated product and sensors.

In summary, we can't really compare those 4 technologies clearly because each technology has different purpose.

Usage

- For Bluetooth is used worldwide included Thailand.
- For Wireless LAN is also worldwide. People use it a lot in Thailand
- For ZigBee use in some country but in different data rate and frequency.
- For WiMax use in some country and in Thailand Chiangmai ,Nakornratchasrima ,Kongran is in during testing invented by True cop.

Cost

- Cost of Bluetooth chip which is around $4.
- The cost of access point is approximately between $800.00 and $2,000.00 per each and The cost of WLAN adapter is range from $200.00 to $700.00.
- The cost of WiMax adapter is around $20 - $299.
- Cost of ZigBee transceiver is around $1 and one radio, processor, memory package is about $3

Reference:

http://moblieZigBee.blogspot.com/2007_08_12_archive.html
http://www.rabbit.com/documentation/docs/manuals/ZigBee/Introduction/glossary.htm
http://www.cs.tut.fi/kurssit/TLT-6556/Slides/4-802.15ZigBee.pdf
http://voip.about.com/od/mobilevoip/a/UsingWiMAXTechnology.htm
http://www.informit.com/library/content.aspx?b=Troubleshooting_Remote_Access&seqNum=19
http://www.cc.kmutt.ac.th/wireless/about.html
http://www.usr.com/download/whitepapers/wireless-wp.pdf
http://www.aha.com/show_apps.php?id=2
http://www.mjtele.com/pds/mjtele_pds/2WP_IEEE802gExpla_12_06.pdf
http://www.radioraiders.com/wlan-datarates.html
http://www.pulsewan.com/data101/wireless_lan_basics.htm
http://www.javvin.com/protocolWLAN.html
http://developers.sun.com/mobility/midp/articles/bluetooth1/
http://www.bluetooth.com/ENGLISH/TECHNOLOGY/Pages/default.aspx
http://www.palowireless.com/infotooth/knowbase/radio/109.asp

Table of Participation

Section	Pongsate Tangseng ID: 5122780786	Witchulada Saetang ID: 5122781503	Kapanai Vimolpatranon ID:5122791494
1. Bluetooth	80		20
2. WLAN	80	20	
3. WiMax		50	50
4. ZigBee		50	50
5. Comparison	33	33	33