CHAPTER 2

LITERATURE REVIEW

2.0 History of Bluetooth

Bluetooth is a low cost, low power, short-range radio technologies intended to replace the cable connections between hand phones, PDAs and other portable devices. It can clean up your desk considerably, making wires between your workstation, mouse, laptop computer and many other devices. Ericsson Mobile Communication started developing their Bluetooth system in 1994, looking for a replacement to the cables connecting their hand phones and their accessories. The Bluetooth system is named after a tenth-century Danish Viking King, Harald Blatand, who united and controlled Norway and Denmark. The first Bluetooth devices hit market around 1999.

Figure 2.1: Bluetooth Official Icon

The Bluetooth SIG is responsible for the further development of the Bluetooth standard. Sony Ericsson, Intel, IBM, Toshiba, Nokia, Microsoft and Motorola are some of the companies involved in the SIG. The composition of the Bluetooth SIG is one of the major strength of the Bluetooth technology. The mixture of both software and hardware supplier participating in the further development of the Bluetooth technology ensures that Bluetooth products are made available to end users. Microsoft support Bluetooth in their Microsoft Windows Operating System. Bluetooth software is made available to the vast majority of the desktop software market. Nokia and Sony

Ericsson include Bluetooth technology in their latest hand phones. This all adds up to a wide availability of the Bluetooth technology for end users. Information of more commercial nature about Bluetooth technology is available on the Bluetooth technology website [1].

2.1 Bluetooth Architecture

The Bluetooth specification aims to allow Bluetooth devices from different manufactures to work with each other, so it is not sufficient to specify just a radio system. Because of this, the Bluetooth specification does not only outline a radio system but a complete protocol stack to ensure that Bluetooth devices can discover, explore and use these services with each other.

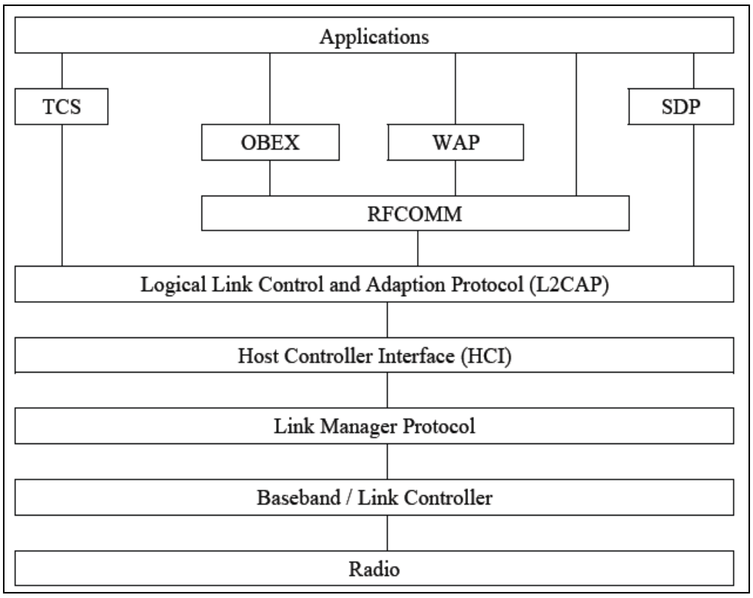

Figure 2.2: The Bluetooth Protocol Stack

The Bluetooth stack is made up of many layers. The HCI is usually the layer separating hardware from software and is implemented partially in software and hardware. The layers below HCI are usually implemented in hardware and the layers above the HCI are usually implemented in software. Table 2.1 gives a short description of each layer shown in Figure 2.2.

Table 2.1: Description of Bluetooth Protocol Stack

Layer	Description
Application	Bluetooth profiles guide developers on how applications should use the protocol stack
Telephony Control System (TCS)	Provides telephony services
Service Discovery Protocol (SDP)	Used for service discovery on remote Bluetooth devices
WAP and OBEX	Provide interfaces to higher layer parts of other communications protocols
RFCOMM	Provides an RS-232 like serial interface
L2CAP	Multiplexes data from higher layers and converts between different packet sizes
HCI	Handles communication between the host and the Bluetooth module
Link manager Protocol	Controls and configures links to other devices
Baseband and Link Controller	Controls physical links, frequency hopping and assembling packets
Radio	Modulates and demodulates data for transmission and reception on air

An understanding of how the Bluetooth radio works is importance. The Bluetooth radio is a lowest layer of Bluetooth communication. The Industrial, Scientific and Medical (ISM) band at 2.4 GHz is used for radio communication. Several technologies used this band as well. For example Wi-Fi technologies like IEEE 802.11b/g and microwave oven may cause interference in this band.

The Bluetooth radio utilizes a signalling technique called Frequency Hopping Spread Spectrum (FHSS). The radio band is divided into 79 sub-channels. The Bluetooth radio uses one of these frequency channels at a given time. The radio jumps from channel to channel spending 625 microseconds on each channel. There are 1600 frequency hops per second. Frequency hopping is used to reduce interference caused by nearby Bluetooth devices and other devices that using the same frequency band.

Adaptive Frequency Hopping (AFH) is introduced in the Bluetooth 1.2 specification and is useful if your devices communicate through both Bluetooth and Wi-Fi simultaneously. The frequency hopping algorithm can then avoid using Bluetooth channels overlapping the Wi-Fi channel in use, hence avoiding interference between your own radio communications.

Every Bluetooth device is assigned a unique Bluetooth address. A 48-bit hardware address equivalent to hardware addresses assigned to regular Network Interface Cards (NIC). The Bluetooth address is used not only for identification, but also for synchronizing the frequency hopping between devices and generation of keys in the Bluetooth security procedures.

2.2 Piconet and Scatternet

A piconet is the usual form of a Bluetooth network and is made up of one master and one slave or more slaves. The device initiating a Bluetooth connection automatically becomes the master. A piconet can consist of a one master and up to seven active slaves. The master device is literally the master of a piconet. Slaves may only transmit data when transmission-time is granted by the master device, also slaves may not communicate directly with each other and all communication must be directed through the master. Slaves synchronize their frequency hoping with the master using the master’s clock and Bluetooth address.

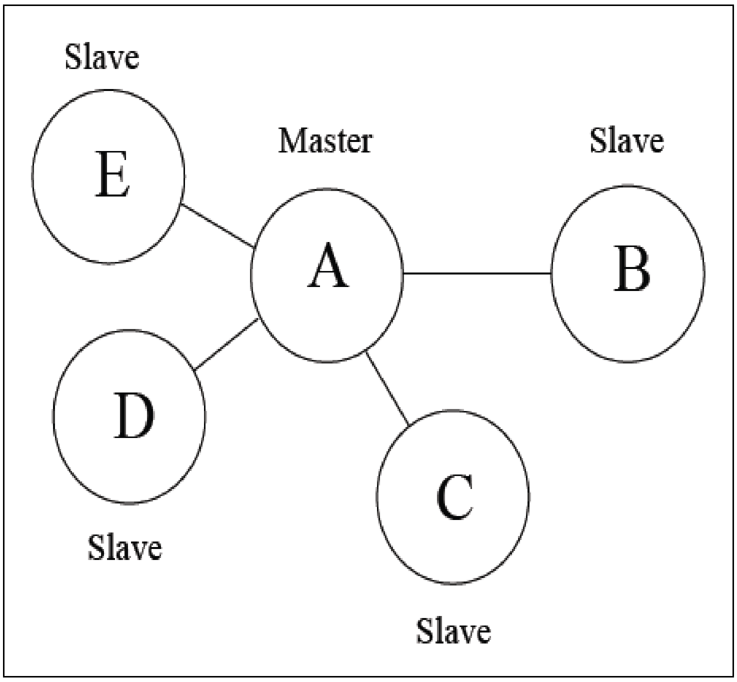

Figure 2.3: The Typical Bluetooth piconet

Piconets take the form of a star network, with the master as the center node, shown in Figure 2.3. Two piconets may exist within radio range of each other. Frequency hopping is not synchronized between two piconets. That means the different piconet only collided on the same frequency.

2.3 Bluetooth links

Two types of physical links are defined in version 1.1 of the Bluetooth specification, Synchronous Connection Oriented (SCO) links and Asynchronous ConnectionLess (ACL) links. The SCO and ACL links are part of the baseband specification.

SCO links are intended for audio transmission. When setting up a SCO link time slots are reserved for transmission of data, thus providing a Quality of Service (QoS) guarantee. Lost or erroneous packages are not re-transmitted which makes sense for voice transmissions. All SCO links operate at 64 kbps. A master device can have up to three simultaneous SCO links at a time, all to the same slave or to different slaves. Slave devices can have up to three SCO links to the Master device.

ACL links are intended for data communication. An ACL link provides error-free transmission of data which means that lost or erroneous packets are re-transmitted. No QoS guarantee is provided. The maximum data rate at the application level is around 650 kbps for an ACL link. A master device can have a number of ACL links to a number of different devices, but only one ACL link can exist between two devices. User data is usually transferred to and from the Logical Link Control and Adaptation Protocol (L2CAP) layer of the Bluetooth stack. Application developers usually refer to L2CAP and RFCOMM links when talking about Bluetooth links. To be precise, L2CAP and RFCOMM are separate layers in the Bluetooth stack which rely on an ACL physical link for data transmission.

L2CAP provides multiplexing between different higher layer protocols over a single physical ACL link, enabling several logical data links to be set up between two Bluetooth devices. L2CAP also provides segmentation and reassembly of packets from higher layers. Different protocols use different packet sizes, some of these may need to be segmented in order to be sent over an ACL link due to package size constraints. An ACL packet can have a maximum of 339 bytes of payload data, while an L2CAP packet can have a maximum of 65,535 bytes of payload data.

The RFCOMM layer emulates RS-232 serial ports and serial data streams. RFCOMM relies on L2CAP for multiplexing multiple concurrent data streams and handling connections to multiple devices. The majority of Bluetooth profiles make use of the RFCOMM protocol because of its ease of use compared to direct interaction with the L2CAP layer.

2.4 Bluetooth device discovery

Due to the ad-hoc nature of Bluetooth networks, remote Bluetooth devices will move in and out of range frequently. Bluetooth devices must therefore have the ability to discover nearby Bluetooth devices. When a new Bluetooth device is discovered, a service discovery may be initiated in order to determine which services the device is offering.

The Bluetooth Specification refers to the device discovery operation as inquiry. During the inquiry process the inquiring Bluetooth device will receive the Bluetooth address and clock from nearby discoverable devices. The inquiring device then has identified the other devices by their Bluetooth address and is also able to synchronize the frequency hopping with discovered devices, using their Bluetooth address and clock.

Devices make themselves discoverable by entering the inquiry scan mode. In this mode frequency hopping will be slower than usual, meaning the device will spend a longer period of time on each channel. This increases the possibility of detecting inquiring devices. Also, discoverable devices make use of an Inquiry Access Code (IAC). Two IACs exist, the General Inquiry Access Code (GIAC) and the Limited Inquiry Access Code (LIAC). The GIAC is used when a device is general discoverable, meaning it will be discoverable for an undefined period of time. The LIAC is used when a device will be discoverable for only a limited period of time.

Different Bluetooth devices offer different sets of services. Hence, a Bluetooth device needs to do a service discovery on a remote device in order to obtain information about available services. Service searches can be of a general nature by polling a device for all available services, but can also be narrowed down to find just a single service. The service discovery process uses the Service Discovery Protocol (SDP). A SDP client must issue SDP requests to a SDP server to retrieve information from the server’s service records.

2.5 Bluetooth versus Wi-Fi

Both Bluetooth and Wi-Fi is a wireless networking technology. Since both technologies is using the same frequency band and share the application, there is a debate going on regarding the merits of these two technologies. In this topic we will discuss the advantages and disadvantage of these technologies. Table 2.2 and 2.3 will briefly explain the comparison between Bluetooth and Wi-Fi technology.

Table 2.2: Advantages of Bluetooth compare to Wi-Fi

Bluetooth	Wi-Fi
Bluetooth components (chips and radios) and device adapters are cheap	WiFi chip and radios is slightly high than Bluetooth
Bluetooth chips have lower power consumption - less drain on battery.	Wi-Fi have high power consumption – battery life and heat is a concern
Bluetooth devices "advertise" their capabilities to others, and a single device can be connected to up to seven other devices at the same time. This makes it easy to find and connect to the device you are looking for or to switch between devices	WiFi is more complex; it requires the same degree of network management as any comparable wired network.

Table 2.3: Disadvantages of Bluetooth compare to Wi-fi

Bluetooth	Wi-Fi
Bluetooth has lower distance range (maximum range is 100m)	Longer distance range (up to 200m)
Bluetooth has generally lower speed in data transfer (1-2 Mbps)	Higher speed in data transfer (11 Mbps- 54 Mbps)

Some say that it not fair to compare the Bluetooth and Wi-Fi technologies. It is because the Bluetooth technology is still new compare to the Wi-Fi. The Bluetooth technology is growing fast. Until this thesis is written, the Bluetooth specification for the version 3.0 and 3.1 is already proposed by the Bluetooth SIG group. For further information reader can refer to Bluetooth SIG website [2].

The main advantages of Bluetooth technology is the lower power consumption and it ease to connect ability. For the Bluetooth 3.0, there the rumours that the Bluetooth will adopt the UWB radio technology. If the Bluetooth SIG can maintain the high frequency using low power consumption, maybe in 10 years the Bluetooth will become the main wireless networking technology.

2.6 Future of Bluetooth

This topic will discuss why the author chooses the Bluetooth technology to develop this project. First of all, over 1 million Bluetooth devices sold worldwide. This becomes the great opportunities to involve in a fast growing technology, where the demand is high for both Bluetooth software and hardware. Lower power consumption in operation make the Bluetooth is suitable for mobile devices. Ease of connection between the devices makes the setting a connection becomes faster and easy.

The Bluetooth technology is growing beyond the limit. So, the author takes these opportunities to do a research about the Bluetooth in the future. This reason becomes a main reason why the Bluetooth is choose as a wireless networking technology to develop this project. Other than that, the ease of connecting between devices and the lower power consumption is a major reason to choose the Bluetooth technology.