FFI-rapport 2015/00293

An introduction to the Bluetooth technology and its applications

Janne M. Hagen and Vinh Pham

FFI Forsvarets forskningsinstitutt

FFI-rapport 2015/00293

An introduction to the Bluetooth technology and its applications

Janne M. Hagen and Vinh Pham

Norwegian Defence Research Establishment (FFI)

21 May 2015

FFI-rapport 2015/00293

1242

P: ISBN 978-82-464-2532-0
E: ISBN 978-82-464-2533-7

Keywords

Trådløs kommunikasjon

IKT

Standardisering

Kommunikasjonsnettverk

Approved by

Ronny Windvik	Project Manager
Anders Eggen	Director

Sammendrag

Blåtann (Bluetooth) er innebygget i ulike produkter. Teknologien er anvendt i helseprodukter, i forretningsprodukter for eksempel logistikk, og selv i sikkerhetsprodukter. I mange tilfeller kan slike blåtannenheter kople seg til mobiltelefoner som ansatte tar med på jobb og på reise. Trenden «bring your own device» (BYOD) kombinert med den store utviklingen når det gjelder sammenkoplede enheter og bærbare kroppsnære elektroniske produkter, også kalt tingenes internett, gjør det nyttig også for Forsvaret å forstå hvordan alle disse tingene koples sammen.

Blåtann muliggjør slik sammenkopling. Vår studie fokuserer på Bluetooth Classic, også kjent som BR/EDR (Basic Rate/Enhanced Data Rate). Bluetooth Classic refererer til eldre versjoner enn Bluetooth 4.0. Vi har valgt å se spesielt på denne versjonen fordi den mellom annet er mye brukt over hele verden. Vårt forskningsspørsmål har vært: Hva er blåtannteknologien, hvordan virker den og hva er anvendelsesområdene? Det følger av forskningsspørsmålet at målet med vår studie er å introdusere blåtannteknologien og dens anvendelser.

Blåtann er teknologi som gjør det mulig å kommunisere trådløst. Standardiseringsarbeidet er ledet av Bluetooth SIG Inc., som har 24 000 bedriftsmedlemmer over hele verden. Disse driver fram blåtannutviklingen. Blant medlemmene finner du store internasjonale maskinvare- og programvareleverandører.

Blåtann bruker radiofrekvenser, og rekkevidden kan være inntil 100 meter avhengig av sendereffekten. Teknologien tillater inntil sju enheter å kople seg til en masterenhet for å bygge såkalte Pico-nettverk, små personlige nettverk. I nyere versjoner av standarden kan flere Pico-nettverk også danne Scatter-nettverk. Teknologien tillater personlige enheter som laptoper, smarttelefoner, ulike bærbare og kroppsnære enheter å kommunisere trådløst. De små nettverkene som skapes, tillater utveksling av filer, lyd, eller å sende dokumenter til utskriving, for å nevne noe. Den brede anvendelsen og den kontinuerlige innovasjonen på området gjør at vi tror at vi vil se enda flere blåtannanvendelser i forbrukerelektronikk og i forretningslivet i framtida.

Karakteristisk for blåtann er at den bruker frekvenshopping, noe som reduserer risikoen for interferens. Men i Scatter-nettverk kan det muligens være en utfordring med interferens fra andre blåtannenheter som ikke har oppdaget andre Pico-nettverk i området. Problemet kan bli større når mengden trafikk i nettverket øker. Det kan føre til at dataraten faller på grunn av pakketap og pakkeretransmisjon. Dersom lyd blir overført og pakker tapes, vil det kunne påvirke kvaliteten på kanalen.

Over tid har imidlertid blåtann forbedret både funksjonalitet, kvalitet og sikkerhet. Sikkerhet har ikke vært et stort tema i denne rapporten, men vil bli grundigere behandlet i en oppfølgingsstudie.

English summary

Bluetooth technology is embedded in various wearables and a variety of consumer electronics. It is used in a range of applications, for instance within health applications, business and even security applications. The devices can often connect to smart phones that employees bring to their offices and on travel. The trend of bringing your own device combined with the big evolution of connecting devices and wearables, also called the Internet of Things, makes it useful also for the defence sector to understand how all these connections and disconnections work. Bluetooth enables such connections. The scope of our study has so far been Bluetooth Classic, which is also known as BR/EDR (Basic Rate/Enhanced Data Rate). Bluetooth Classic refers to versions prior to Bluetooth 4.0. We have chosen this scope because this version seems to be widely disseminated worldwide. The research question we ask is: *What is Bluetooth technology, how does it work and which are the user applications?* Naturally, it follows that the objective of this study is to introduce Bluetooth technology and its applications in general.

Bluetooth is a technology that enables wireless communication. The Bluetooth standard is managed by Bluetooth SIG Inc., which has 24000 member companies worldwide that jointly drive the Bluetooth developments. Among these you find huge international hardware and software producers.

The Bluetooth technology allows two Bluetooth enabled devices to wirelessly communicate with each other. Bluetooth uses RF technology, and the radio range can reach up to 100 meters depending on the power. It also enables up to seven devices to connect to a master device and builds a so-called Piconet of the connected devices. In newer versions, several Piconets can merge into Scatternets. Thus, the technology enables personal devices such as laptops, smartphones, various wearables etc. to wirelessly connect together, forming a small wireless network providing a number of applications ranging from file transfers, music listening, printing of documents etc. Its applications are wide and continuously growing, and that is why we can expect to see even more applications in consumer electronics, transportation and more in the future.

One of the characteristics of the Bluetooth technology is its use of frequency hopping, which reduces the risk for interference. However, in a Scatternet there may be interference from other Bluetooth devices that are not aware of other Piconets in the area. The result may be frequent packet loss and reduced packet throughput. The problem can escalate as the density of Piconets and Bluetooth devices in a given area increase, and consequently increased traffic, resulting in increased interference and further decrease in throughput. If voice traffic experiences frequent packet loss, the result may be poorer voice quality on the communication channel.

The Bluetooth evolution shows, however, that over time, both functionally and security has improved. Security has not been a major topic in this first introductory report, but it is our intention to study the security aspects in a follow-up study.

Contents

Preface

Bluetooth is a standard for wireless low range communication that has existed for quite many years. It is applied in a variety of consumer electronics, which are often also connected to smart phones. With the trend of interconnection of devices to the Internet, the Internet of Things, Bluetooth might be even more relevant and reach an even broader dissemination worldwide. In 2014 Bluetooth hits 90 percent penetration in all mobile phones.

In this report we give a first introduction to the standard and the technology. Our ambition is to provide an overview introducing the Bluetooth technology, how it works and some of its applications to the reader. Security is not much discussed in this report but will be covered in a follow up study.

This report is written in English because the literature and the terminology is in English. It makes it easier for potential readers to search for updates on the topic on the Internet.

Kjeller 11.02.2015

Janne Hagen and Vinh Pham

1 Introduction

1.1 Background

Bluetooth is a standard for interconnection and data exchange named after Harald Bluetooth, the king of Denmark in the late 900s (Curt and Layton, 2014). Many manufacturers are making devices that use Bluetooth technology to enable wireless communication. These devices include mobile phones, personal digital assistants (PDAs), laptops, printers, automobiles, and medical devices enabling users to form ad hoc networks to transfer voice and data. It is reported that the annual Bluetooth product shipments surpass 2.5 billion[1].

Bluetooth is managed by Bluetooth SIG Inc., which has more than 24,000 member companies that jointly drive the Bluetooth development. To market Bluetooth devices, manufacturers must be members of the SIG and their products must pass the Bluetooth Qualification Program, which ensures compliance to requirements of the Bluetooth specification. In 2014 Bluetooth hits 90 percent penetration in all mobile phones.

The Bluetooth technology relies on short-range radio frequency. Any device that incorporates the technology can communicate as long as it is within the required distance. The technology is used to allow two Bluetooth enabled devices to communicate with each other without the need for wiring. For example, you may be able to operate your computer with a wireless keyboard, use a wireless headset to talk on your mobile phone, or add an appointment to your friend's PDA calendar from your own PDA.

The advantages of Bluetooth include: wireless communication, simple to use, and inexpensive. There are other ways to get around using wires, including infrared communication (IR). But, infrared (IR) is a "line of sight" technology and it is almost always a "one to one" technology. You can send data between your desktop computer and your laptop computer, but not your laptop computer and your PDA at the same time. Bluetooth bypasses these limitations.

Over time the Bluetooth standard has evolved from a simple low-speed cable replacement technology to become a multiservice, multimedia wireless interconnection standard[2]. The application of Bluetooth is expected to increase in accordance with the evolution and the feasibility of the technology, and with the development of the Internet of Things. In this context, the motivation of this report is to provide an introduction to the Bluetooth technology and its applications.

1.2 Research Questions

The objective of this study is to produce a brief overview of Bluetooth technology and its applications.

[1] http://www.bluetooth.com/Pages/History-of-Bluetooth.aspx

[2] Lawrence Harte, “Introduction to Bluetooth. Technology, Market, Operation, Profiles and Services,” 2nd edition, Althos Publishing, 2010.

The scope of the study is confined to Bluetooth Classic, which is also known as BR/EDR (Basic Rate/Enhanced Data Rate), and refers to versions prior to version Bluetooth 4.0. This is a deliberate choice due to several reasons:

- The Bluetooth Standard has evolved over time since its birth and includes many versions. The first version is 1.0 while the latest is 4.1. A complete overview to all these versions is beyond the scope, time frame and the size of this report.
- We choose to narrow this introduction to Bluetooth Classic as this is a very popular and widespread version. Bluetooth Classic is also the original and fundamental version in which later versions of Bluetooth are more or less based on or derivated from.
- Bluetooth Classic is more complex and has more functionality compared to other version such as Bluetooth Low Energy (LE). An understanding in Bluetooth Classic allows for easier transition to other Bluetooth versions.
- Bluetooth Classic is more versatile in terms of applications. On the other hand Bluetooth LE is targeted at more specific applications, namely ultra-low power consumption, and exchange of low-bandwidth data that are sent occasionally.
- Even though Bluetooth LE inherits a number of functionality from Bluetooth Classic, and thus has some similarities, it is however very different from its predecessors. While previous versions focused on enhancing the throughput, Bluetooth LE takes an entirely new direction, i.e. minimizing power consumption drastically. In order to achieve this goal, several key components in the protocol stack have been redesigned from scratch. Due to the major differences between the two versions in terms of application and architecture, it may be more appropriate to describe and discuss Bluetooth LE in a separate report.

The report address the below listed research question:

What is Bluetooth technology, how does it work and which are the user applications?

1.3 The Report Outline

The rest of the report is structured like this:

- Chapter 2 introduces applications of Bluetooth technology
- Chapter 3 gives an overview of our chosen methodology for the study.
- Chapter 4 describes in brief the evolution of Bluetooth and how the standard has improved over time.
- Chapter 5 introduces Bluetooth technology and how it works, its protocols and how devices establish a connection.
- Chapter 6 presents the architecture of Bluetooth.
- Chapter 7 summaries the answer to our research question.

2 Which are the Applications?

Since its invention, the Bluetooth technology has gradually gained widespread proliferation. It is now the de-facto standard short range wireless communication technology. Bluetooth can now be seen in a number of applications, ranging from industrial automation, health-care, and transportation to mention a few areas. The following subsections provide examples of typical Bluetooth applications.

2.1 Bluetooth in Industrial Automation

The origin of Bluetooth goes back to 1998 and the aim of the technology was to replace connecting cables with a cost-effective wireless communication method. Many of the engineers who developed Bluetooth came from an industrial automation background and they knew the importance of making Bluetooth technology robust and reliable for industrial applications.

Bluetooth has a determined set of “profiles” that in essence are application defined behaviors that Bluetooth devices use to communicate with each other. Important profiles used in industrial applications of Classic Bluetooth include the following:

- Serial Port Profile (SPP), is used during data exchange between computers, control systems, and other devices with a serial interface and emulates a complete serial interface with hardware handshaking via Bluetooth. A traditional serial interface (UART, RS232, RS422, or RS485) can be replaced with a wireless point-to-point, point-to-multipoint, or multi-drop connection.
- Personal Area Network (PAN) can be used to transmit IPv4 and IPv6 protocols transparently. Supported are both ad-hoc and access point operations. PAN is ideal for Ethernet-compatible devices with small amounts of data. In addition, PAN can also provide local access to the machine and system network during configuration and maintenance.[3]

Schneider Electric UK is a worldwide supplier of products and services for Power and Control that has developed a Bluetooth management system, enabling operators to manage pole mounted Remote Terminal Unit (RTU) from the safety of ground. The operator connects a Bluetooth enabled PC to the RTU, which integrates an OEM Serial Port Adapter from connectBlue. The operator can then upgrade software, reconfigurations and run diagnostics on site, but from a distance of up to 100 meters[4].

[3] Rolf, Nilssen, Industrial wireless: Bluetooth can be robust, easy to use, Control Engineering, 02/25/2013, http://www.controleng.com/single-article/industrial-wireless-bluetooth-can-be-robust-easy-to-use/cbd481b6e65b08d2e743f8e09fb95528.html, downloaded 25th August 2014.

[4] Ublox, ConnectBlue, Wireless Industrial Automation, http://www.connectblue.com/applications/wireless-industries/industrial-automation/ , downloaded 25th August2014.

2.2 Temporary Applications

Bluetooth piconets provide flexibility and scalability in addition to temporary communications when needed. Bluetooth replaces cables. It makes it easier to share files with devices within the same piconet. Bluetooth can also provide automatic synchronization, for instance calendars and address books between Bluetooth enabled devices in the same piconet, such as laptops. Finally, Bluetooth with internet connectivity can share access with other Bluetooth devices, for instance a laptop can use a mobile phone to establish an internet connection through the phone (Padgette, Scarfone and Chen, 2012).

Some examples are:

- Connections between mobile phone and wireless headset, tablets and speakers such as iPad and Android devices
- Connections between PC input and output devices such as mouse, keyboard and printer

2.3 Health-sector

The company A&D has been providing sensors for telemedicine applications for more than a decade. Their experience in the transfer of vital signs to external systems for post processing began as a joint development project with leading companies in Japan in the early 90's. Theirs products include among others blood pressure meters and weigh scales using Bluetooth.[5] Ahmed et al (2014) discusses another Bluetooth application; e-Health monitoring. Their case is a connected personal health device (wearable), a blood pressure monitor, with a user's smartphone. It provides the patient with direct supervision and control. Hugo et al (2012) provides another example by using an implanted glucose monitor device sending signals to a wearable, for example a wrist watch, and to an Ambient Assisted Living Program on a PC. The system provides better supervision and control of the blood-sugar of the patient.

Additional numbers of devices that you may already use take advantage of this same radio-frequency band. Baby monitors, garage-door openers and the newest generation of cordless phones all make use of frequencies in the ISM band. Making sure that Bluetooth and these other devices don't interfere with one another has been a crucial part of the design process (Curt and Layton, 2014).

2.4 Transportation

Bluetooth technology has been used in logistics for a while. Tarn et al (2009) points to the applications of Bluetooth in shipping. In particular the contribution of Bluetooth technology to the package shipping industry is significant, as Bluetooth products have increased the effectiveness for the companies when it comes to tracking and control. Well-known companies like FedEx, UPS and DHL have applied Bluetooth with great success.

[5] A&D Medical, Products, http://www.telemedicine.jp/products.html, downloaded 25th August 2014.

Bluetooth and Wireless LAN products are also found in buses of main public transportation companies in Italy and France. When a bus returns to the depot, the system wirelessly downloads data via the on-board Serial Port Adapter to a Communication Controller in the depot. Diagnostic reports, statistics of operations and predictive diagnosis is processed by the back office software, installed in the central server in ATM’s data center. Thereby, a holistic view of the state of the vehicle is provided to the operator.[6]

Bluetooth enabled hands-free calling systems are included as standard equipment on millions of new cars and trucks. All 12 of the world's major car manufacturers offer Bluetooth hands-free calling systems in their vehicles.[7] Being able to connect a Bluetooth device to the car's audio system enables the driver to securely use the Bluetooth device while driving. Automakers are getting involved in the effort to get smartphone apps running in the car. Even consumer electronics makers such as Pioneer and Sony are getting in on the apps-in-the-car market, adding the ability to connect phones to their latest car receivers. These systems allow drivers to run apps they might find useful while driving, sending information from their phone to their car's flat-panel display and audio system. These apps are helpful to drivers like locating the cheapest gas or playing of streamed music over the Internet via the phone on long road trips. Many car navigation systems also include Bluetooth hands-free calling[8].

“Bluefly” is an integrated cockpit avionics system that uses Bluetooth. Bluefly allows pilots to use their mobile devices to instruct the aircraft to fly different routes, avoid bad weather and communicate with air traffic control. Pilots tap their finger to request take off or see visual depictions of system health during an emergency.[9]

2.5 Various Consumer Electronics

Internet of things (IoT) has huge potential for wireless communication. According to an article written by Rolf Nilsson (2014) as much as 90% of the market will be in the last 100 meters. This means great opportunities for the Bluetooth technology, but the technology faces competition from other communication technologies like LTE, NFC, RFID and Wi-Fi, to mention a few. The number of personal devices such as smartphones, tablets, laptop are limited to the number of people using devices. Therefore Nilsson says that the greatest growth will be seen in IoT devices. Numbers varies between 25 and 50 billion devices, and they will disseminate through sectors like energy, transportation, education, health care, commerce, travel and tourism, finance, IT, and

[6] Ublox, ConnectBlue and digigroup, “Public transportation Wireless Communication,” http://www.connectblue.com/applications/wireless-industries/professional-vehicles/digigroup/ downloaded 25th August 2014.

[7] Automotive market rapidly expanding beyond hands-free calling, http://www.bluetooth.com/Pages/Automotive-Market.aspx, downloaded 15.03.14

[8] Bluetooth Technology Transforming Consumer Electronics, Blueetoth.com, Automotive market rapidly expanding beyond hands-free calling, Bluetooth.com, http://www.bluetooth.com/Pages/Automotive-Market.aspx, downloaded 09.09.2014

[9] Bluetooth Smart Allows Pilots to Control Airplanes with Smart Devices, Posted on February 10, 2015 by Nanci Taplett, http://blog.bluetooth.com/bluetooth-smart-allows-pilots-to-control-airplanes-with-smart-devices/?_ga=1.42807522.655795211.1390289816, downloaded 11.02.2015.

environment (Nilsson, 2014). New innovations are also coming. Examples are the hi-Call glove (from a company named hi-Fun) has a speaker built into the thumb and a microphone in the pinky, so you can talk by making the traditional "call me" hand[10], and a footwear that uses Bluetooth to signal the user's mobile phone's mapping system to navigate. It can help joggers from getting lost.[11] Nordic Conductor has developed a chip that uses the Bluetooth Smart standard. Last year they sold more than 1 billion chips. The chips are used in watches that register heart beat signals measured on the wrist, or while sitting in the sofa and watching TV, sending signals between the remote control and the TV set.[12]

The vast consumer electronics market today is filled with opportunities for Bluetooth technology, with countless devices consumers can use in their home, their car, or on the go. ABI Research forecasts for instance over 3 billion Bluetooth enabled devices are shipped in 2014, and by 2018 there will be over 10 billion enabled devices in the market[13]:

- In 2014, IHS forecasts 90% of all mobile phones will be Bluetooth enabled, growing to 96% by 2018
- The Bluetooth enabled wireless audio market is forecasted to grow to more than 250 million units by 2018
- Approximately 1.4 billion Bluetooth Smart compatible smartphones and tablets are forecasted to be shipped in 2014 alone. That number will grow to over 2.1 billion units in 2018
- There are more than 10 billion wirelessly connected devices in the market today. By 2020, this is expected to reach over 30 billion presenting a huge opportunity for Bluetooth enabled CE devices

According to market research firm ABI Research, nearly two billion smart phones will be shipped globally by 2018, almost tripling the amount for all of 2011, as millions of consumers buy cheaper and faster smartphones.

There is also a fast-growing demand for phone apps that can capture and process new types of information from Bluetooth sensors. Demand for apps is especially high in sports & fitness and health & wellness. For example, apps that collect workout data from wireless heart-rate monitors, foot pods, cycling computers, and other exercise devices and display it on a phone or PC, upload it to the web, and let consumers share their workouts and results with friends.

[10] Talk to Your Hand with Bluetooth, Posted on August 29, 2012 by Bluetooth SIG, http://blog.bluetooth.com/talk-to-your-hand/comment-page-1/#comment-125, nedlastet 15th March 2014.
[11] Now, bluetooth enabled footwear to help joggers from getting lost ANI | London April 15, 2014 Last Updated at 14:58 IST. http://www.business-standard.com/article/news-ani/now-bluetooth-enabled-footwear-to-help-joggers-from-getting-lost-114041500673_1.html, downloaded 15 April 2014.
[12] Ingvild, Buaset, Staker inn med norsk børsvinner, Oppdatert: 13.feb. 2014 17:56, http://www.aftenposten.no/okonomi/Staker-inn-med-norsk-borsvinner-7467623.html#.U2htUWw4UdV, downloaded 6 May 2014.
[13] http://www.bluetooth.com/Pages/Consumer-Electronics-Market.aspx, downloaded 09.09.2014.

The same Bluetooth technology powering the latest wireless sports and fitness devices helps diabetics monitor blood sugar and send the information to healthcare providers, or helps monitor blood pressure and other vital signs from home or anywhere, using small wireless devices. Demand is expanding for both the apps and devices to support these new uses of Bluetooth technology.

Bluetooth is also used in security products. By the use of The Kwikset Kevo, you can easily lock and unlock your door by the use of your smartphone and Bluetooth.[14]

And, if you are not satisfied with your default Bluetooth Android app, it is developed a more advanced one, provided by Medieval Software. You can share whichever kind of format, and manage them from the app. By using the app you can share audio, video and image, also inside Zip, and you can compress and extract zipped files, create screen folders, streaming, file sort, bookmarks among others. It also supports multiple languages.[15]

3 Methodology

3.1 Research Scope

Research questions determine the research strategies and methodologies. In this study we explore the Bluetooth technology with emphasis on Bluetooth Classic. We have therefore applied an exploratory and qualitative research design. The report aims to provide a brief description of Bluetooth technology by introducing to the reader the basic technology concepts and the applications.

Our scope is Bluetooth Classic, i.e. prior versions of Bluetooth before version 4.0, which is the most commonly used version. At the same time our focus is directed towards Bluetooth functionality and architecture. We have not focused on Bluetooth security in this report, since it will be covered in a separate security study.

3.2 Literature Review

We have performed a literature review based on books, by searching the Internet and research databases for Bluetooth technology documents. There exists a variety of sources with different quality. The literature sources used in this report is briefly summarized below:

- The Bluetooth Core specification version 4.1.
- Books on Bluetooth technology.
- Peer reviewed papers – in this category there are PhD and Master Dissertations, and scientific papers.

[14] http://www.kwikset.com/kevo/default.aspx#.VQqxpI6G-mg
[15] http://www.appszoom.com/android_applications/communication/bluetooth-file-transfer_fmm.html?ref=list_referer

- Internet resources – associations and open sources, blogs etc. Among others, the website www.bluetooth.org is maintained by Bluetooth SIG and is dedicated to members and serves as the definitive source of information around Bluetooth programs, initiatives, and Bluetooth wireless technology development.

4 The Evolution of Bluetooth

4.1 Key Differences between Bluetooth Classics and Bluetooth Low Energy

In this report we focus on Bluetooth Classic. The key differences between Bluetooth Classics (also called BR/EDR) and Bluetooth Low Energy (LE) are summarized in Table 4.1 (Padgette, Scarfone and Chen, 2012). Bluetooth LE has reduced functionality, lower data rate and much lower power consumption compared with the Bluetooth Classic (BR/EDR). Additional differences can be read from Table 4.1.

Table 4.1 The key characteristics of Bluetooth BR/EDR and LE

Characteristics	Bluetooth BR/EDR	Bluetooth LE
RF Physical Channels	79 channels, 1 MHz channel spacing	40 channels, 2 MHz channel spacing
Discovery/Connect	Inquiry/Paging	Advertising
Number of Piconet slaves	7 active and 255 inactive devices Supports Scatternet	Unlimited, Does not support Scatternet
Device Address Privacy	None	Private Device Addressing Available
Max Physical Data Rate	1-3 Mbps	1 Mbps via GFSK modulation
Max Throughput	0.7-2.1 Mbps	0.27 Mbps
Encryption Algorithm	E0/SAFER+	AES-CCM
Typical Range	30 m	50m
Max Output Power	100 mW (20 dBm)	10 mW(10dBm)

4.2 A Brief Overview of Improvements over Time

Bluetooth has evolved over time. Newer versions come with improved functionality and security compared to older versions. Below, we outline the evolution of Bluetooth technology in brief and some of the main differences between the different versions of Bluetooth[16]:

Bluetooth v1.0 and v1.0B were the first versions, and they had problems regarding interoperability and anonymity. Versions 1.0 and 1.0B also included mandatory Bluetooth hardware device address (BD_ADDR) transmission in the Connecting process

[16] Bluetooth, http://en.wikipedia.org/wiki/Bluetooth, downloaded 26thAugust 2014.

(rendering anonymity impossible at the protocol level), which was a major setback for certain services planned for use in Bluetooth environments.

Bluetooth v1.1 was ratified as IEEE Standard 802.15.1 in 2002. This version of the specification added possibility for non-encrypted channels and Received Signal Strength Indicator (RSSI).

Bluetooth v1.2 added Adaptive frequency-hopping spread spectrum (AFH). This mechanism provides improved resistance to radio frequency interference by avoiding the use of crowded frequencies in the hopping sequence. In addition, higher transmission speeds and improved voice quality of audio links by allowing retransmissions of corrupted packets were provided. It was ratified as IEEE Standard 802.15.1 in 2005.

Bluetooth v2.0 + EDR was released in 2004. The main difference is the introduction of an Enhanced Data Rate (EDR) for even faster data transfer. EDR can provide lower power consumption through a reduced duty cycle.[17]

Bluetooth v2.1 + EDR was adopted by the Bluetooth SIG in 2007. Secure simple pairing (SSP) was included and also "Extended inquiry response" (EIR), which provided more information during the inquiry procedure to allow better filtering of devices before connection. Low-power mode was introduced.

Version 3.0 + HS of the Bluetooth Core Specification was adopted by the Bluetooth SIG in 2009. Bluetooth 3.0+HS provides 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 collocated 802.11 link. The main new feature is AMP (Alternative MAC/PHY), the not mandatory addition of 802.11 as high speed transport. Alternative 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 alternative 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 faster radio is used when large quantities of data need to be sent.

Bluetooth 4.0: The Bluetooth SIG completed the Bluetooth Core Specification version 4.0 (called Bluetooth Smart/Smart Ready) and has been adopted as of 30 June 2010. It 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 4.1 was adopted in December 2013. This specification is an incremental update to Bluetooth Specification v4.0. The update incorporates Bluetooth Core Specification Addenda (CSA 1, 2, 3 & 4) and adds new features which improve consumer usability with increased

[17] See http://en.wikipedia.org/wiki/Bluetooth#cite_note-21

co-existence support for LTE, bulk data exchange rates, and aid developer innovation by allowing devices to support multiple roles simultaneously.

5 Introduction to the Bluetooth Technology

Bluetooth is a standard for short-range, low-power, and low-cost wireless technology that enables devices to communicate with each other over radio links. As already mentioned in the introductory chapter Bluetooth was originally invented to replace serial data cables. However, the technology enables personal devices such as laptops, smartphones, headsets etc. to wirelessly connect together, forming a small wireless network called Wireless Personal Area Network (WPAN). Within this network, Bluetooth provides a number of applications ranging from file transfers, streaming of music, printing of documents, and making mobile calls on Bluetooth headsets, car audio systems and more.

5.1 Bluetooth Topology

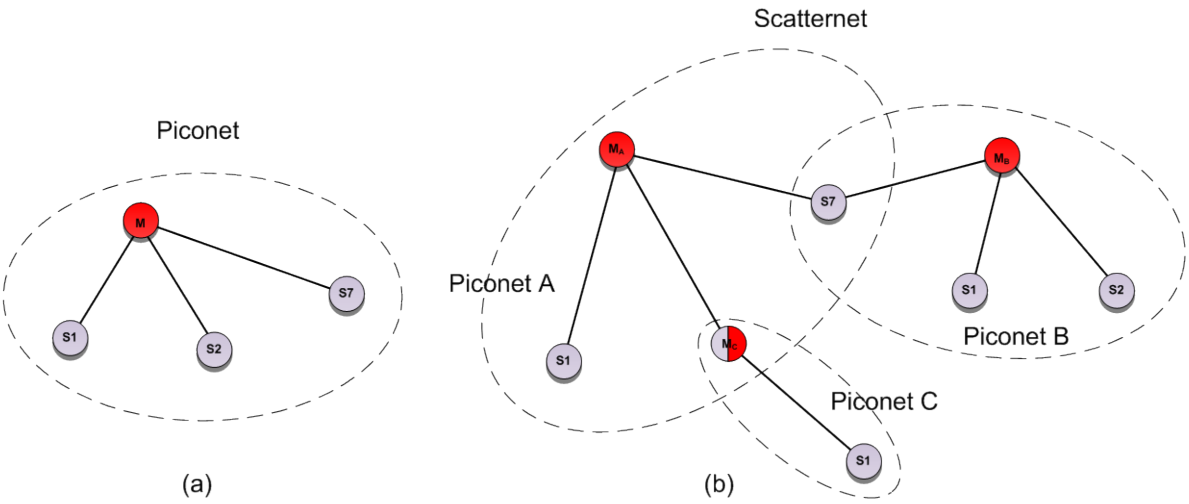


Figure 5.1 (a) Piconet (b) Scatternet

Bluetooth can be used to form a network of interconnected Bluetooth devices. The smallest network is called a piconet as shown in Figure 5.1 (a) and consists of a master node (red circle denoted M) and up to 7 active slave nodes (grey circle denoted S). All nodes in the piconet are synchronized with each other in terms of clock and frequency hopping pattern. The master's clock is used as the reference clock in the piconet, and the frequency hopping pattern is calculated based on the master's Bluetooth device address (BD_ADDR) and clock. Within a piconet, only a master and a slave can communicate directly to each other. Direct communication between two slaves is not possible. If two slaves need to communicate, they can disconnect from their respective piconets and form a separate piconet with one of them acting as the master and the other as slave.

Several piconets may co-exist in proximity to each other without interfering with each other. This is because each piconet will have its own master and thus its own frequency hopping pattern.

A scatternet is a network consisting of two or more piconets that are hierarchically connected together as shown in Figure 5.1 (b). A node that is member in two different piconets may either be slave in both as in the case of node S7, or slave in one and master in the other piconet, as in the case of node M_C. It is not possible for a node to be master in two piconets since a piconet is defined by the master’s BD_ADDR and clock. All nodes that are synchronized with a master node form one single piconet and not two different piconets. Furthermore, a node that participates in two piconets does that in a Time Division Multiplexing (TDM) manner, i.e. it participates in one piconet for a certain amount of time and then participates in the second piconet for the remaining time.

5.2 Time Division Duplex and Frequency Hopping

The physical channel is divided into time slots where each slot is 625 μs as shown in Figure 5.2. Channel access is based on a polling-scheme in which the master polls or asks a slave if there is any traffic to send. Upon receiving a poll message, the slave can send a packet in the immediately following time slot. The communication between the master and a slave thus occurs in slot pairs, i.e. the master first transmits a packet, and then it is the receiving slave's turn to reply. In order to poll a slave, the master may either send a POLL message if itself has no data to send, or alternatively, it can send a data packet, that implicitly serves as a POLL message. This polling-based channel access scheme allows the master to take the complete control of who can access the channel and when it can be accessed.

A packet from master-to-slave and a reply from slave-to-master may occupy 1, 3 or 5 time slots depending on the packet type and length, as shown in Figure 5.2. An important rule to notice is that a master can only begin to send a packet in even time slots, while a slave can only begin to respond in odd time slots.

Frequency Hopping Spread Spectrum (FHSS) is used to provide some protection against interference. This means that each packet transmission occurs on different frequency channel following a pseudo-random hopping pattern. There are in total 79 channels of 1 MHz bandwidth, ranging from 2402 GHz to 2480 GHz. The basic frequency hopping occurs at a rate of 1600 hops/second. Note from the figure that a packet that occupy 3 or 5 time slots, is sent on the channel defined by the initial time slot, for the whole duration of the packets. For example, the packet from slave 2 to the master is sent in the time slot 3-5, and the channel in which the packet is sent on is f(3), see Figure 5.2 below. In other words, the channel is defined by the time slot in which the packet transmission/reception begins.

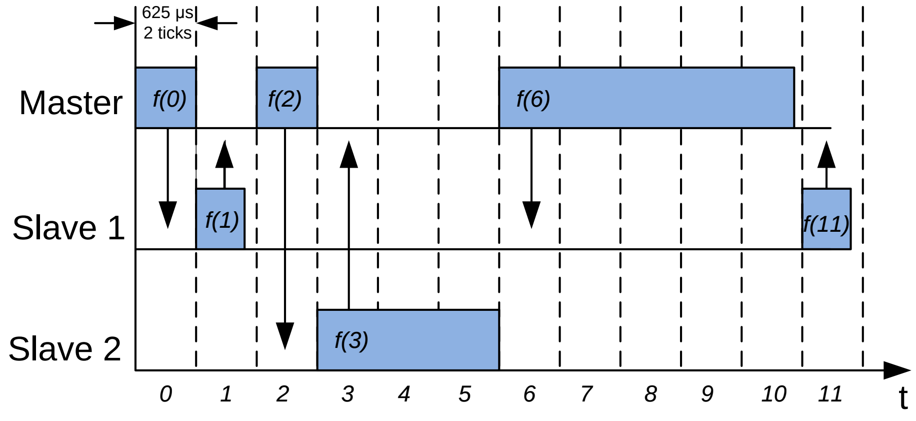


Figure 5.2 Time Division Duplex and Frequency Hopping Spread Spectrum

In terms of protection against eavesdropping or traffic sniffing, even though it is possible with specialized hardware such as Ubertooth[18], Frontline's BPA 600[19] or Ellisys's Bluetooth Explorer 400[20], the fact that Bluetooth utilizes a pseudo random frequency hopping pattern makes it much more challenging to eavesdrop. In contradiction, other wireless technology such as Wifi, which does not utilize frequency hopping but transfer data traffic on the same frequency all the time, is far easier to eavesdrop.

5.3 Modes

5.3.1 Discoverable

Bluetooth devices use a procedure called Inquiry to discover nearby devices. A Bluetooth device that tries to find other nearby devices is known as the inquiring device, and will actively send Inquiry requests, asking "Hello, is there anyone here". A Bluetooth device that is configured to be in discoverable mode, listen for these Inquiry requests and sends Inquiry responses telling the inquiring device about its presence. Non-discoverable devices, on the other hand, will just ignore Inquiry requests. For security reasons, most Bluetooth devices are by default in the non-discoverable mode. The inquiring process is described in more detailed in subsection 5.8.

5.3.2 Connectable

Bluetooth devices use a procedure called Paging to establish a connection with each other. A Bluetooth device that wants to establish a connection to another device will actively send Page requests. Upon reception of the request, the paged device, if configured to be in the connectable mode, sends a response back to the paging device. The two devices will then continue the page procedure to establish a connection. Following a successful conclusion of the page procedure, both devices are connected to each other, and are thus synchronized with each other in terms of

[18] http://ubertooth.sourceforge.net/
[19] http://www.fte.com/products/BPA600.aspx
[20] http://www.ellisys.com/products/bex400/

timing and hop frequency pattern. They form a piconet in which the initiator the paging device, by default, is the master and the paged device is the slave. In the case if the paged device is non-connectable, it simply just ignores any page request. The paging process is described in more detailed in subsection 5.8.

5.3.3 Bondable

Bluetooth devices use a procedure called Pairing to establish a trusted relationship with each other. A pairing procedure typically takes place after a paging procedure, and involves verifying a shared secret in form of a PIN-code. Following a successful conclusion of the pairing procedure, both devices share a secret common link key that can be used for authentication as well as derivation of encryption keys, etc. When a Bluetooth device is in bondable mode it will accept a pairing request that results in bonding. Devices in non-bondable mode will ignore any paring request.

5.4 Bluetooth Device Address

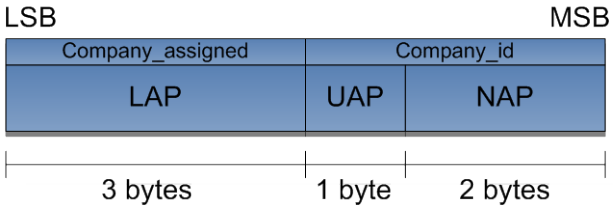


Figure 5.3 Bluetooth Device Address (BD_ADDR)

Each Bluetooth device has a globally unique 6 bytes or 48 bits long Bluetooth device address (BD_ADDR) as shown in Figure 5.3. It is similar to the MAC-address of an Ethernet network interface, and is in fact, administered by the same organization IEEE[21]. The address consists of 3 fields: Lower Address Part (LAP), Upper Address Part (UAP) and Non-significant Address Part (UAP). The most significant 24 bits of the address, i.e. UAP and NAP together, identify the manufacturer, and is also referred to as Organizationally Unique Identifier (OUI). The least significant 24 bits of the address, i.e. the LAP field, is assigned by the manufacturer to each Bluetooth device.

The Bluetooth device address plays a rather important role in term of security due to the following reasons:

- The frequency hopping pattern of a particular piconet is derived from the BD_ADDR and the clock of the master. Thus, without the knowledge about these parameters it is not possible to synchronize and follow the hopping pattern nor eavesdrop traffic from the piconet.

[21] Naresh Gupta, “Inside Bluetooth Low Energy,” Artech House, Boston, London, 2013.

- Once the BD_ADDR of a target device is known, it is more susceptible for information harvesting from potentially hostile devices. For instance, a device will respond on information queries directly addressed to it (using the tools: *hcitool info* or *sdptool browse*), even though it is in non-discoverable and non-connectable mode.

Due to these reasons, the BD_ADDR of a device is seldom revealed in clear text.

5.5 Packet Format

The generic Bluetooth Classic Packet Format is shown in Figure 5.4 and comes in two flavors, BR and EDR. The difference is that an EDR packet has a Guard and a Sync field before the payload, and a Trailer after the payload. This is because EDR packets use a different modulation scheme, i.e. Differential Phase Shift Keying (DPSK), in order to achieve higher data rate for the payload. These fields are necessary to facilitate the change in modulation scheme just before the payload is transmitted or received. Note that the initial fields of the EDR packet is always sent using the BR modulation, i.e. Gaussian Frequency Shift Keying (GFSK).

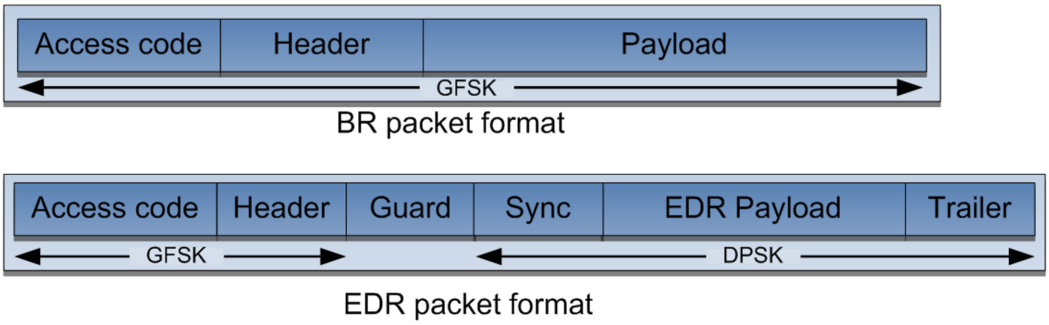


Figure 5.4 BR and EDR packet format

5.5.1 Access Code

A Bluetooth packet always begins with an access code, which is the only mandatory part. The remaining fields of the packet are optional. The access code is used for synchronization, DC offset compensation, and identification.

There are defined 3 different access codes:

1. Device Access Code (DAC)
2. Channel Access Code (CAC)
3. Inquiry Access Code (IAC)

All access codes are derived from the LAP of a Bluetooth device address or an Inquiry address. DAC is used during paging and is derived from LAP of the paged device, i.e. the slave. This allows a master to send a directed connection request to a unique target slave. CAC is used as a unique identifier for a piconet, and is derived from the LAP of the master’s LAP. All packets exchanged in a piconet share the same unique CAC. Finally, the IAC is used during the inquiring procedure. Unlike, the former to access codes, the IAC is derived from reserved and dedicated LAPs. The IAC is thus used to broadcast information not to a specific target device but to all devices in the vicinity. A more detailed description of the inquiry and paging procedure is provided in subsection 5.8.

5.5.2 Packet Header

The header contains link control information as shown in Figure 5.5. It consists of 6 fields:

- Logical transport address (LT_ADDR), used to identify the slave (in both cases as receiver or sender)
- Packet type indicates the packet type
- The Flow bit is used for the purpose of traffic flow control to prevent buffer overflow
- The ARQN bit is used to piggyback an acknowledgement to inform the source of a successful transfer of the recently received packet
- The SEQN bit provides a sequential numbering scheme to order the data packet stream
- The 8 bit Header Error Check (HEC) field is used to check the header integrity

The total length of the header is 18 bits. Before concatenating the header to the packet, the header is further encoded with 1/3 Forward Error Correction (FEC) resulting in a 54-bit header.

3	4	1	1	1	8 (bits)
LT_ADDR	Type	Flow	ARQN	SEQN	HEC

Figure 5.5 Packet Header format

5.6 Packet Types

Bluetooth packets can be classified into 3 categories:

1. Link Control Packets
2. ACL Packets
3. SCO Packets

Link control packets are special signaling packets, and there are defined 5 link control packets:

- The ID (Identity) packet is used before connection establishment. It is a very short and hence a robust packet. The length is only 68 bytes, and contains the device access code (DAC) or inquiry access code (IAC).
- The NULL packet has no payload and is generally used for acknowledgement or to indicate the buffer status. It is typically used when a slave receives a packet from the master in which it has to acknowledge, but has no data to transfer. In addition, the slave may also use the NULL packet to notify the master that its buffers are full. The master will then defer further transmissions until the slave has emptied its buffer.

- The POLL packet also has no payload. It is used by the master to check the presence of the slaves and secondly to check if they have any data to send. When receiving a POLL packet, a slave must respond with an acknowledgment. If the slave does not have any data to send, it responds to the master with a NULL packet.
- The FHS (Frequency Hop Synchronization) is a special control packet used to inform the recipients about the sender's BD_ADDR and clock. Prior to sending a FHS packet, the clock information must be updated. The information provided in the FHS packet is essential for nodes to synchronize with each other in terms of clock and frequency hop sequence.
- The DM1 (Data Medium Rate 1-slot) packet is used by the Link Manager and Link Controller (also called Baseband) to exchange control packets. In addition to carrying control packets, this packet can also be used to carry regular data.

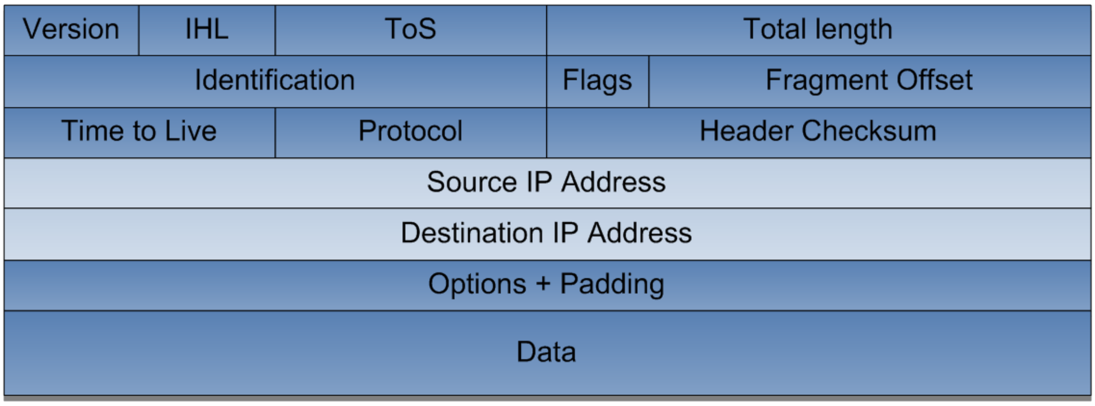
Asynchronous Connection Oriented (ACL) packets are used to transport *data only traffic* over an ACL link, i.e. a connectionless, packet switched link. ACL packet typically is designated as DM or DH. An example of ACL packet is DM1 which means "Data packet, Medium Rate, 1 Slot". The packet is sent over 1 time slot. On the other hand a DH5 packet means "Data packet, High Rate, 5 Slot", which is sent over 5 time slots and provides higher data rate.

Synchronous Connection Oriented (SCO) packets are typically used to transport *voice/audio traffic* or a combination of voice and data over a SCO link, i.e. a point-to-point, circuit switched link. Examples of SCO packets are HV, meaning "High Quality Voice" and EV "Enhanced Voice". In addition, there is also a DV packet type, meaning "Data-Voice" which can transport both data and voice traffic simultaneously. However, this latter packet type is seldom used (Gupta, 2013).

5.7 Bluetooth Packet vs. IP Packet

Comparing a Bluetooth packet with an IP-packet as shown in in Figure 5.4 and Figure 5.6, respectively, one major difference is that a Bluetooth packet does not contain any explicit information about the source and destination address like in the case of an IP-packet. Instead, a Bluetooth packet uses the access code to identify the destination physical channel or piconet. In addition the LT_ADDR field in the packet header (Figure 5.5) is used to address a particular destination node part of the piconet. When the master sends a packet to a slave, the LT_ADDR represents the destination slave. When a packet is sent in the direction slave to master, the LT_ADDR represents the source slave.

The access code is derived from the BD_ADDR of the master node. On the other hand the LT_ADDR is an ID that is assigned by the master to a node when it becomes an active slave. The fact that packet addressing is based on access code and LT_ADDR instead of using the BD_ADDR explicitly is also a factor that makes Bluetooth more resilient against eavesdropping[22] [23]. Without knowledge about the BD_ADDR of the master node, it is not possible to determine the frequency hopping pattern of a particular piconet, nor sniffing its traffic.



<table>
<tr><td>Version</td><td>IHL</td><td>ToS</td><td colspan="2">Total length</td></tr>
<tr><td colspan="3">Identification</td><td>Flags</td><td>Fragment Offset</td></tr>
<tr><td colspan="2">Time to Live</td><td>Protocol</td><td colspan="2">Header Checksum</td></tr>
<tr><td colspan="5">Source IP Address</td></tr>
<tr><td colspan="5">Destination IP Address</td></tr>
<tr><td colspan="5">Options + Padding</td></tr>
<tr><td colspan="5">Data</td></tr>
</table>

Figure 5.6 IP-packet Format

5.8 Connection Establishment

5.8.1 Inquiry

Inquiry is the process of discovering nearby Bluetooth devices within the radio range. When a Bluetooth device A wants to establish a piconet, it has to first discover other Bluetooth devices in its neighborhood. Device A then sends inquiry messages asking “Hello is anyone here”. Another node, for example device B, that hears this message, may send an inquiry response back to device A if it is in *discoverable* mode. Since the inquiring node does not know which channel other devices are listening on, the inquiry messages are sent on multiple channels. The message rate is 3200 packets/s, i.e. two times per time slot, each on different channels. The message exchange is as follows:

1. Inquiry request (ID from master to slave)
2. Inquiry response (FHS from slave to master)

5.8.2 Paging

Once a Bluetooth device knows the address of another device it can connect to the remote device using the paging procedure. The paging procedure is initiated by the initiator node sending a page request message (ID packet). The receiving node then replies with a page response message if it is *connectable*, meaning that it allows other nodes to connect to it. The initiator who sends the page request is by default the master node, while the responding node who accepts the connection request is the slave. However, the master and slave roles may be switched at a later time after the connection has been established.

[22] Dominic Spill and Andrea Bittau, “BlueSniff: Eve meets Alice and Bluetooth,” WOOT '07 Proceedings of the first USENIX workshop on Offensive Technologies, 2007

[23] http://ubertooth.blogspot.no/

The page request contains a Device Access Code (DAC) which is derived from the target node's LAP. Since the master does not know which channel the target slave is listening on, it repeatedly sends multiple page request messages on different channels in order to assure that the slave receives the page message. Like the inquiry request, the page requests are sent at the rate of 3200 packets/s, i.e. two times per time slot, each on different channels.

Once a connection is established, the slave is synchronized in terms of frequencies and clock timing with the master, and they can send/receive packets to/from each other. The whole paging procedure is as summarized below:

1. Page request (ID from master to slave)
2. First slave page response (ID from slave to master)
3. Master page response (FHS from master to slave)
4. Second slave page response (ID from slave to master)
5. First Master packet (POLL from master to slave)
6. First Slave packet (No data: NULL. Have data: ACL, SCO or eSCO. From slave to master)
7. Data exchange between master and slave in both directions

6 Bluetooth Architecture Overview

6.1 Bluetooth Protocol Stack

Bluetooth has a layered architecture. At a high-level the architecture may be depicted as shown in Figure 6.1, consisting of lower and upper layers, profiles and applications. The lower layers or the controller are responsible for low level operations like discovering devices in the vicinity, making connections, exchange of data packets, security and power management etc. The functionality of the lower layers is generally implemented in a Bluetooth chip.

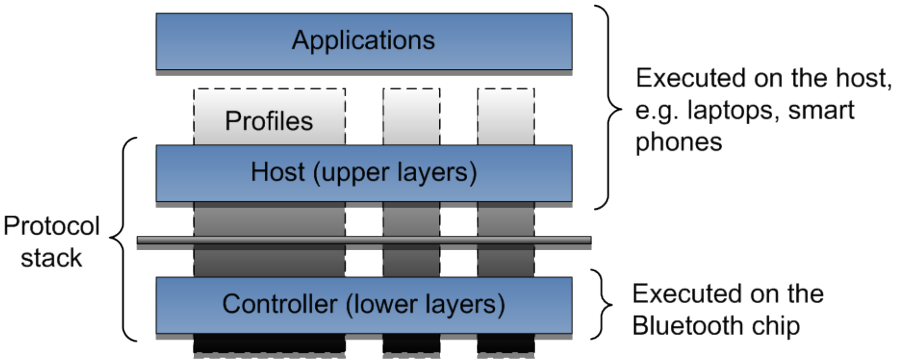

Applications
Profiles
Host (upper layers)
Controller (lower layers)
Protocol stack
Executed on the host, e.g. laptops, smart phones
Executed on the Bluetooth chip

Figure 6.1 High-level representation of the Bluetooth architecture.

The upper layers make use of the functionality provided by the lower layers to provide more complex functionality. Examples are serial port emulation, transferring big chunks of data by

Profiles may be considered as vertical slices through the protocol stack. They specify how each of the protocol layers come together to implement a specific usage model. Profiles ensure that application implementations from different vendors are interoperable. Examples of profiles include File Transfer Profile (FTP), Advanced Audio Distribution Profile (A2DP) for distribution of high-quality audio, and Serial Port Profile (SPP) for serial port emulation.

Bluetooth applications are the user interfaces that allow the end-user to make use of the Bluetooth functionality. Examples of such applications are: File browsing and transferring, streaming of audio/voice, searching for other Bluetooth devices in the vicinity, etc. The upper layers and applications are implemented and executed on the host, e.g. laptops and smart phones.

The Bluetooth technology was designed with the aim to reuse as much as possible of available standards instead of designing everything from scratch. Some useful components from existing standards were adapted as needed and reused. The remaining components of the protocol stack were designed from scratch. The proprietary Bluetooth components are referred to as core protocols while reused components are referred to as adopted protocols.

Figure 6.2 shows a detailed representation of the Bluetooth architecture. The figure illustrates that the Bluetooth architecture is made of a mixture of core and adopted protocols. In addition, the figure also shows a subset of defined profiles. Note that even though this figure contains more details compared to Figure 6.1, the shown components represent just a subset of all components that the Bluetooth architecture is made of. It is beyond the scope of this introduction to cover the complete Bluetooth technology, but rather to give an initial insight of it. The following subsections are devoted to explain some of the components in the architecture in more detail.

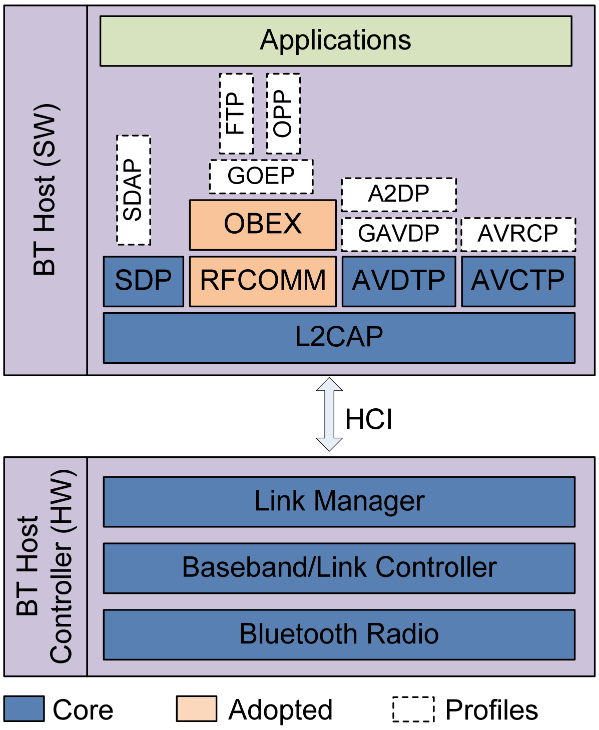


Figure 6.2 A detailed representation of the Bluetooth architecture

6.2 Bluetooth Radio

The Bluetooth Radio is responsible for transmission and reception of packets over radio frequency. It operates in the 2.4 GHz ISM band which is the same band as many other user electronics including Wifi, the microwave oven, cordless telephones etc. [24] To mitigate the risk for interference, the Bluetooth Radio therefore uses Frequency Hopping Spread Spectrum (FHSS). Instead of using a constant frequency to send and receive data, the communicating devices use a set of frequencies and hop rapidly from one frequency to another using a pseudo random pattern.

In order to support two way communications, i.e. full duplex transmission, a Time Division Duplex (TDD) scheme is used. The usage of both FHSS and TDD implies that packets are transmitted in defined time slots and on defined frequencies.

The Bluetooth Radio can support two types of modulation[25]:

1. Basic Rate (BR): This mode is mandatory and must be supported by all Bluetooth versions. BR uses a shaped binary FM modulation mechanism and provides a gross air data rate of 1 Mbps.
2. Enhanced Data Rate (EDR): This mode is optional and uses Phase Shift Keying (PSK) modulation and supports higher data rates. The gross air data rate supported is 2 Mbps or 3 Mbps.

Furthermore, 3 power classes are defined in order to accommodate various requirements in terms of radio range. Higher output power results in longer radio range as shown below:

1. Power Class 1: Maximum output power 100 mW. Radio range ≈100 m
2. Power Class 2: Maximum output power 2.4 mW. Radio range ≈10 m
3. Power Class 3: Maximum output power 1 mW. Radio range ≈1 m

6.3 Baseband

The Baseband controller (also called Link Controller) is responsible for the following major functions:

- Management of physical channels and links
- Selection of the next hopping frequency for transmitting and receiving packets
- Formation of piconet and scatternet
- Creation of packets
- Inquiry and Inquiry Scan

[24] http://en.wikipedia.org/wiki/Electromagnetic_interference_at_2.4_GHz

[25] Naresh Gupta, “Inside Bluetooth Low Energy,” Artech House, 2013

- Connection and Page Scan
- Security, including encryption
- Power management

Some of these functions are discussed in detail below.

6.4 Link Manager

The Link Manager is responsible for link set-up and link control, and includes:

- Procedures for creation and removal of a connection
- Security procedures which include authentication, pairing, and encryption.
- Information exchange, e.g. about version, supported features, etc.
- Control of power modes and duty cycles of the Bluetooth radio
- Quality of service (QoS) with respect to bandwidth allocation

6.5 Host Controller Interface

The Host Controller Interface (HCI), see Figure 6.2, provides a communication interface between the Host and the Controller. It is the interface between the higher and the lower layers of the Bluetooth stack and provides a uniform method for the host to access the controller's capabilities. One of the strength of the Bluetooth specification is this well-defined interface which allows for independent and parallel development of the host and controller. The advantage of this is that a host from one vendor can work beautifully together with a controller from another vendor. For example a Bluetooth dongle from any vendor can be plugged into a PC to use the Bluetooth functionality. All communications over the HCI interface happens in form of packets. The host sends HCI command packets to the controller to instruct it to perform a desired task. The controller, on the other, hand asynchronously notifies the host about the status and results of the current task by using HCI event packets. In addition to control messages, both ACL and SCO/eSCO data packets can also be exchanged in both directions between host and controller using the HCI interface.

6.6 Logical Link Control and Adaptation Protocol

The Logical Link Control and Adaptation Protocol (L2CAP) is located above the Baseband layer and provides connection-oriented and connectionless data services to the upper layers in the Bluetooth protocol stack. A connection-oriented channel is used to transport point-to-point data between two devices, while a connectionless channel is used for broadcasting data to multiple receivers. The L2CAP Specification is defined for only ACL links and no support for SCO links is planned. L2CAP is responsible for the following major functions:

- Managing the creation and termination of logical links for each connection through “channel” structures
- Provides Quality-of-Service (QoS) on data flows

- Allows higher level protocols and application to transmit and receive L2CAP data packets up to 64 kB. However, since a baseband packet can at most transport 1021 bytes, the L2CAP-layer needs to adapt the upper-layer data to the baseband formats through Segmentation and Reassembly (SAR)
- Performing Multiplexing of higher-level protocol data to support multiple concurrent connections over a single common link

6.7 Service Discovery Protocol

The Service Discovery Protocol (SDP) is a protocol used to discover the services provided by a remote device and the characteristic and supported profiles of those services. As an example, a laptop wants to play an audio file on a Bluetooth wireless speaker. It will first send an Inquiry message to discover nearby Bluetooth devices. In the next step, it connects to these devices to search for the services provided by these devices. In order to play audio, it will search for a device that provides Advanced Audio Distribution Profile (A2DP) service. Once such a device is found, it may create an A2DP connection with that device to play the file.

6.8 Radio Frequency Communication

The Bluetooth protocol Radio Frequency Communication (RFCOMM) is a simple set of transport protocols, located on top of the L2CAP protocol, which emulates the RS232 serial port. Recall that one of the original purposes of the Bluetooth technology was to replace the serial cable and RFCOMM is the key component to enable this replacement. The Bluetooth *serial port profile* (SPP) is based on this protocol. Many Bluetooth applications use RFCOMM because of its widespread support and publicly available Application Programming Interface (API) on most operating systems.

RFCOMM supports up to 60 simultaneous connections between two Bluetooth devices, allowing multiple separate applications to run and exchange data in parallel. The RFCOMM protocol is an adopted protocol and is based on the ETSI standard TS 07.10.

6.9 Object Exchange Protocol

The Object Exchange Protocol (OBEX) is a communication protocol that facilitates the exchange of binary objects between devices. The protocol is adopted from the Infrared Data Association (IrDaA). OBEX utilizes the client/server model and is applied in many Bluetooth profiles to exchange (push/pull) or synchronize data object such as business cards, notes, images, files, calendars etc. The format for these objects are standardized and are referred to as vCard, vCalendar, vMessage, and vNotes

6.10 Profiles

Bluetooth profiles can be considered as vertical slices through the protocol stack and define the vertical interactions between the layers as well as the peer-to-peer interactions of specific layers between devices. A profile provides information on how each of the protocol layers comes together to implement a specific usage model. It defines the features and functions required from each layer of the protocol stack from Bluetooth Radio, Baseband, up to L2CAP, RFCOMM, OBEX etc. In addition, application behaviors and data formats are also defined by the profile. Bluetooth profiles are built upon the Bluetooth protocol stack and while the Bluetooth specifications define how the technology *works*, profiles define how it's *used*. The purpose of the profiles is to ensure that the technology is easy to use and that it is used correctly. Profiles are essential in terms of application interoperability, i.e. they help to guarantee that an implementation from one vendor will work properly with an implementation from another vendor.

Currently, there are more than 30 profiles defined in the Bluetooth specification. The Generic Access Profile (GAP) is a base profile that all Bluetooth devices must support. A device typically supports several profiles at the same time. What profiles it supports determine what application it is designed for. A hands-free Bluetooth headset, for example, would use headset profile (HSP), while a Nintendo Wii Controller would implement the human interface device (HID) profile. For two Bluetooth devices to be compatible, they must support the same profiles.

7 Conclusion

In this study we raised the research question: *What is Bluetooth technology, how does it work and which are the user applications?*

Bluetooth is a technology that enables wireless communication. The Bluetooth standard is managed by the Bluetooth SIG Inc. The technology allows two Bluetooth enabled devices to wirelessly communicate with each other. Bluetooth uses RF technology and the typical range is between 10-100 m, depending on the output power configuration. It enables up to 7 devices to connect to a master device and build so called Piconets among the connected devices. In newer versions, several Piconets can merge into Scatternets. Thus, the technology enables personal devices such as laptops, smartphones, headsets and other wearables etc. to wirelessly connect together, forming a small wireless network providing a number of applications ranging from file transfers, listening of music, printing of documents etc. Its applications are wide and continuously growing, and that is why we can expect to see it in many applications, including consumer electronics, transportation, health care etc.

One of the characteristics of the Bluetooth technology is its use of frequency hopping, which reduces the risk for interference. However, in a Scatternet, there may be interference from other Bluetooth devices in other Piconets, which are not aware of other Piconets in the area. The result may be frequent packet loss and reduced packet throughput. The problem will escalate as the density of Piconets and Bluetooth devices in a given area increase, resulting in increased interference and further decrease in throughput.

The Bluetooth evolution shows that over time, both functionally and security has improved. Security has not been a major topic in this report, but it is our intention to study security aspects in the follow-up study.

References

J. Padgette, K. Scarfone, L. Chen, “Guide to Bluetooth Security. Recommendations of the National Institute of Standards and Technology”, NIST Special Publication 800-121 Revision 1, June 2012

A&D Medical, Products, Home page, http://www.telemedicine.jp/products.html, downloaded 25th August 2014.

Ahmed, S, Sayakkare, A., Kim, G. and D. Kim, “Self-organized e-Health Application using IEEE 11703: An Experimental Approach”, *Procedia Computer Science* **32** (2014): 876-881.

“Automotive market rapidly expanding beyond hands-free calling”, http://www.bluetooth.com/Pages/Automotive-Market.aspx, downloaded 15.03.14.

Bluetooth Specification, Version 4.1 [Vol 1], Architecture & Terminology Overview, 03. December 2013: 17.

“Bluetooth Technology Transforming Consumer Electronics, Automotive market rapidly expanding beyond hands-free calling”, Bluetooth.com, http://www.bluetooth.com/Pages/Automotive-Market.aspx, downloaded 09.09.2014.

Buaset., I, «Staker inn med norsk børsvinner», Oppdatert: 13.feb. 2014 17:56, http://www.aftenposten.no/okonomi/Staker-inn-med-norsk-borsvinner-7467623.html#.U2htUWw4UdV, downloaded 6 May 2014.

“Consumer Electronics Market, Transforming Consumer Electronics”, Home page, www.Bluetooth.com, http://www.bluetooth.com/Pages/Consumer-Electronics-Market.aspx, downloaded 06.02.2015.

Franklin, C, and J. Layton. "How Bluetooth Works", Electronics.com, http://electronics.howstuffworks.com/bluetooth.htm, downloaded 06.02.2015.

Gupta, N., *Inside Bluetooth Low Energy*, Artech House, London, Boston, 2013.

Harte, L., “Introduction to Bluetooth. Technology, Market, Operation, Profiles, and Services, 2nd Edition”. *Althos Publishing*, Fquay – Varina, USA.

“History of the Bluetooth Special Interest Group”, Home page, http://www.bluetooth.com/Pages/History-of-Bluetooth.aspx, downloaded 06.02.2015.

“Kwikset Kevo review: This brainy smart lock just isn't brawny enough”, Review, www.cnet.com, http://www.cnet.com/products/kwikset-kevo-bluetooth-door-lock, downloaded 02142014.

Lawrence, H., “Introduction to Bluetooth. Technology, Market, Operation, Profiles and Services”, 2nd edition, *Althos Publishing*, 2010.

Lund, E., "More files and formats to share via bluetooth", Reviewed May 25, 2011, http://www.appszoom.com/android_applications/communication/bluetooth-file-transfer_fmm.html?ref=list_referer, downloaded 06.02.2015.

Nilsson, R., “Technology Update: Connectivity of things:
Wireless for the last 100 m of IoT,” *Control Engineering*, March 2014: 16., http://www.controleng.com/single-article/industrial-wireless-bluetooth-can-be-robust-easy-to-use/cbd481b6e65b08d2e743f8e09fb95528.html, downloaded 06.02.2015.

Now, Bluetooth enabled footwear to help joggers from getting lost, London April 15, 2014 Last Updated at 14:58 IST. http://www.business-standard.com/article/news-ani/now-bluetooth-enabled-footwear-to-help-joggers-from-getting-lost-114041500673_1.html, downloaded 15 April 2014.

Public Transportation Wireless Communication, Home Page, Ublox, http://www.connectblue.com/applications/wireless-industries/professional-vehicles/digigroup/, downloaded 25th August 2014.

Talk to Your Hand with Bluetooth, Posted on August 29, 2012 by Bluetooth SIG, http://blog.bluetooth.com/talk-to-your-hand/comment-page-1/#comment-125, nedlastet 15th March 2014.

Taplett, N., Bluetooth Smart Allows Pilots to Control Airplanes with Smart Devices, Posted on February 10, 2015, http://blog.bluetooth.com/bluetooth-smart-allows-pilots-to-control-airplanes-with-smart-devices/?_ga=1.42807522.655795211.1390289816, downloaded 11.02.2015.

Tarn, J. M., Pang, C., Yen, D. and J. Chen, “Exploring the implementation and application of Bluetooth technology in the shipping industry”, *Computer standard and Interfaces*, **31** (2009): 48-55.

Abbreviations

A2DP	Advanced Audio Distribution Profile
ACL	Asynchronous Connection Oriented
API	Application Programming Interface
BD_ADDR	Bluetooth Device Addres
BR	Basic Rate
CAC	Channel Access Code
DAC	Device Access Code
DPSK	Differential Phase Shift Keying
EDR	Enhanced Data Rate
FEC	Forward Error Correction
FHS	Frequency Hop Synchronization
FHSS	Frequency Hopping Spread Spectrum
FTP	File Transfer Profile
GAP	Generic Access Profile
GFSK	Gaussian Frequency Shift Keying
HCI	Host Controller Interface
HEC	Header Error Check
IAC	Inquiry Access Code
IoT	Internet of Things
L2CAP	Logical Link Control and Adaptation Protocol
LAP	Lower Address Part
LT_ADDR	Logical Transport Address
NAP	Non-significant Address Part
OBEX	Object Exchange Protocol
OUI	Organizationally Unique Identifier
QoS	Quality of Service
RFCOMM	Radio Frequency Communication
RSSI	Received Signal Strength Indicator
SAR	Segmentation and Reassembly
SCO	Synchronous Connection Oriented
SDP	Service Discovery Protocol
SPP	Serial Port Profile
TDD	Time Division Duplex
TDM	Time Division Multiplexing
UAP	Upper Address Part
Wi-Fi	Wireless Fidelity