Rapport Bluetooth technology
Gioacchino Brucato 2mmp (pdt)
English miss Bogaert
“Connections between people are changing as an ever-increasing number of wireless products enable them to enjoy mobility and simplicity without cabling. Introduced in 1998 and evolving, Bluetooth® is a low power, short-range radio technology that revolutionizes communications for a wide array of products from mobile phones to computer peripherals. An open specification, Bluetooth offers convenience, enhanced immunity from interference and security which have made it the choice of a large and growing number of companies. In this paper we will talk about how Bluetooth is conceived, how it works and what makes it the best wireless connection.”
# Table of contents

1. Introduction
   1.1 Bluetooth technology p4
   1.2 Bluetooth Special Interest Group p4
   1.3 About the name and logo p5

2. Bluetooth technology explained
   2.1 Bluetooth Networking p5
   2.2 Range p5
   2.3 Bluetooth Components p6
   2.4 Bluetooth Terminology p6
      2.4.1 Bluetooth stack p7
      2.4.2 Links and channels p8
   2.5 Security p8

3. Conclusion p9

4. Graphical glossary p10

5. Non-graphical glossary p11

6. References p12
1. Introduction

1.1 Bluetooth technology

Bluetooth is an open standard specification for a radio frequency based, short-range connectivity technology. Bluetooth changed the face of computing and wireless communication. Bluetooth is a low power 2.4 GHz radio technology that eliminates cables between electronic devices such as phones, computers, keyboards, mouse products, printers and other equipment. Bi-directional radio transmission between these devices delivers physical freedom and ease of use through automatic wireless connections. Up to 7 devices may be connected in a piconet, the fundamental Bluetooth network. One of the strengths is the ability to simultaneously handle data and voice transmissions. Currently Bluetooth specification v2.1 is used and the maximum data rate is 3 Mbps, with typical performance in the range of 1 Mbps. Bluetooth 3 is developing and will provide a data rate up to 480 Mbps and will use less power.

The idea of a cable-free, or wireless, technology was initially conceived by Ericsson in 1994. The company began a study of a low-power, low-cost radio interface between mobile phones and their accessories. The company’s goal was to eliminate the need for cables. The original Bluetooth specification was developed by Jaap Haartsen, a Dutchman, who worked for Ericsson. The idea was to create a small, inexpensive radio chip that could be used in mobile computers, printers, mobile phones and so on, to transmit data between these devices. The radio chip would replace cables. The projected cost of the chip was around $5. The chip used low power so that it could be used in devices that rely on battery life.

Bluetooth is now used in many different products by many different manufacturers. These manufacturers must be members of some level in the Bluetooth Special Interest Group before they are granted access to the Bluetooth specifications. The Bluetooth specification defines a uniform structure for a wide range of devices to connect and communicate with each other. The SIG also specifies a qualification process that products must be tested before they may be branded with the Bluetooth trademarks and sold to consumers. It also markets the Bluetooth brand and technology and owns the trademarks and standardization documents.

1.2 Bluetooth Special Interest Group

The Bluetooth Special Interest Group (SIG) is a privately held, not-for-profit trade association. The Special Interest Group was founded in September 1998, consisted of five companies: Ericsson, IBM, Intel, Nokia en Toshiba. Four other major companies (Microsoft, 3Com, Lucent and Motorola) later joined this founding group to form the Bluetooth Promoter Group. Many more companies have since become part of the Bluetooth revolution, expanding on the original vision and helping drive the development of this new technology. The Bluetooth SIG itself does not make, manufacture or sell Bluetooth enabled products. The Bluetooth SIG is now comprised of more than 10 000 member companies. Any company incorporating Bluetooth wireless technology into its products, must become a member of the Bluetooth Special Interest Group.

Bluetooth SIG members are key to the success of Bluetooth wireless technology because they influence its direction and development. As Bluetooth wireless technology is an open platform, all members of the Bluetooth SIG have permission to use Bluetooth wireless technology in their products and services. The Special Interest Group has a small group of dedicated staff in Hong Kong, Sweden and the USA. In addition to the Bluetooth SIG staff, volunteers from member companies play key roles in furthering Bluetooth wireless technology and the organization behind it. Members support a number of working groups and committees that focus on specific areas, such as engineering, qualification and marketing. SIGnature is the award-winning publication from the Bluetooth Special Intrest Group. The quarterly magazine serves as a paper, helping our more than 10 000 member companies expand and refine the Bluetooth wireless brand.
1.3 About the name and logo

For those who know little about the technology, and even for those who are more than a little acquainted with it, the name Bluetooth may seem odd. You may wonder in fact, how it is related to wireless technology. Or speculate that perhaps it’s derived somehow from the founding members of the Bluetooth SIG. Neither of these ideas is correct. The name is a romantic gesture that in some sense indicates the excitement the technology generates as well as the belief in its value as a revolutionary concept.

To combine these qualities in a name, required ingenuity and delving into the past. The name Bluetooth comes from Danish history. Harald Blatand, who was called Bluetooth, was the son of King Gorm the Old, who ruled Jutland, the main peninsula of Denmark. By the time Harald became king, he was a skilled Viking warrior. When his sister, after her husband died, asked for help to secure control in Norway. Harald quickly seized the opportunity to unite the countries and expand his kingdom. By 960 A.C. according to the story, Harald was at the height of his powers and ruled both Denmark and Norway. He was later credited with bringing Christianity to his Viking realm. Although it was popularly believed that King Harald had a blue tooth. It’s more likely that the Bluetooth name is the English derivative of the original Viking word, Blatand. The Bluetooth name was chosen for the wireless technology because its developers and promoters hope it will unite the mobile world, just as King Harald united his world.

A Scandinavian firm originally designed the logo at the time the SIG was formally introduced to the public. Keeping to the same origin as the Bluetooth name, the logo unites the Runic alphabetic characters “H”, which looks similar to an asterisk, and a "B”, which are the initials for Bluetooth. If you look close enough you can see both symbols in the logo.

2. Bluetooth Technology explained

2.1 Bluetooth Networking

The Bluetooth technology provides both a point-to-point connection and a point-to-multipoint connection. In point-to-multipoint connections, the channel is shared among several Bluetooth units. In point-to-point connections, only two units share the connection. Any Bluetooth device can be a master or a slave, depending on the application scenario. Bluetooth employs frequency hopping spread spectrum (FHSS) to communicate. Bluetooth radio modules avoid interference from other signals by hopping to a new frequency after transmitting or receiving a packet. So in order for multiple Bluetooth devices to communicate, they must all synchronize to the same hopping sequence. The master sets the hopping sequence and the slaves synchronize to the master. A piconet or Bluetooth network is formed by a master and up to seven active slaves. The slaves in a piconet only communicate with the master. This means slaves can’t communicate one another. A scatternet can be formed by linking two or more piconets. When a device is present in more than one piconet, it must synchronize to the master of the piconet with which it is currently communicating. While the topology and hierarchical structure of WLAN networks are relatively simple, Bluetooth networks are far more diverse and dynamic. They are constantly being formed, modified and dissolved. Bluetooth devices move in and out of range of one another. And because different Bluetooth devices can represent many different usage profiles, there are many different ways in which Bluetooth devices can interact.

2.2 Range

Bluetooth devices are grouped into three power classes or levels with typical operating range distances of 10 m, 20 m and 100 m. Most keyboards and mouse products operate at the 10 or 20 meter ranges. The actual effective range for any device may be less, as radio signals can be affected by the physical environment. Since keyboards are generally used within a building, which attenuates radio signals, the actual range could be less
than 10 m. A consideration for using Bluetooth in offices is that the range may extend through a floor or ceiling. Many Bluetooth radios have an active transmit power control feature. If the keyboard is moved closer to the transceiver, the two radios will reduce transmission power accordingly so that they are not transmitting any louder than necessary. This further reduces the effective range, but helps to minimize potential interference with other networks.

2.3 Bluetooth Components

A complete Bluetooth system will require these elements:

A Radio Frequency portion for receiving and transmitting data
A Module with a baseband microprocessor
A Memory
An Interface to the host device (such as a mobile phone)

This basic system will vary, depending on whether the Bluetooth module is independent of the host or embedded. First, consider the module scenario. The RF portion can be implemented as a module or as a single chip. Ericsson has a module available that includes a short-range radio transceiver, an external antenna and a clock reference (required for synchronization). It can be used independently or with a baseband module, which Ericsson also offers.

Other transceivers also are available for Bluetooth applications. Those transceivers also can be used with another company’s baseband solution or with a packaged baseband processor. In this type of arrangement, the lower-layer Bluetooth protocols are supported in the baseband module and the host processor must support the upper-layer protocols. In other words, the RF-baseband solution provides the means to communicate with the host, but you need to implement a connection interface, as well as any upper-layer protocols, to use applications supported by the final product. The upper layers of the technology support what are known as the Bluetooth profiles. In other words, a set of protocols is optimized for a class of applications, for example, dial-up networking or file transfer. This feature is important, because it enables interoperability among devices. Requiring a specific profile for devices that provide comparable applications ensures interoperability across a spectrum of devices.

Another option for manufacturers is to embed a fully integrated RF-baseband Bluetooth chip. In this scenario, the upper-layer protocols reside within the single chip, freeing the host processor from the protocol processing. The cost of the chip necessarily will be higher, but the fully integrated final design can be less complex, use less power and reduces production cost. In this scenario, the Bluetooth unit can connect to the host device through a serial interface such as a universal serial bus (USB).

Yet another possibility for implementing Bluetooth is to integrate the Bluetooth baseband module with the host system. This option would involve owning and customizing the silicon chip for the device. In this case, the device manufacturer would have complete control of interfaces and features for the device, but development costs and investment risk could be high.

2.4 Bluetooth Terminology

The Bluetooth specification, while innovating, does not define a totally new technology. In fact, Bluetooth draws heavily on existing radio communications and networking technologies, which enables it to be operationally compatible with the existing devices that also use these technologies. Many of the various terms and concepts used in Bluetooth are borrowed from other technologies and are included in the specification of Bluetooth’s elements, such as baseband, radio frequency communications and many of the protocols. What makes Bluetooth unique is how it applies its proprietary components and the existing technologies to define its central core operations and its application profiles. Regardless of their source, the components that are integral to Bluetooth are worth examining a little more closely.
2.4.1 Bluetooth stack

As already noted, the baseband, or radio module, is the hardware that enables wireless communication between devices. The building block of this technology is the Bluetooth stack, which includes the hardware and software portions of the system. The Bluetooth stack has the following components:

- Bluetooth Radio Frequency for reception and transmission signals (RF)
- Bluetooth Baseband with microcontroller
- Link controller unit and link manager to support lower-layer protocols (LMP)
- Host controller interface (HCI)
- Logical link control and adaptation protocol to support upper-layer protocols (L2CAP)

The radio frequency portion provides the digital signal processing component of the system and the baseband processes these signals.

The link controller handles all the baseband functions and supports the link manager. It sends and receives data, identifies the sending device, performs authentication and determines the type of frame to use for sending transmissions. The link controller also directs how devices listen for transmissions from other devices and can move devices into power-saving modes.

The link manager is located on top of the link controller. It’s responsible for the creation, modification and release of logical links as well as the update of parameters related to physical links between devices. The link manager achieves this by communicating with the link controller. In remote Bluetooth devices the link management protocol (LMP) is used. The baseband and the link manager together establish connections for the network.

The host controller interface communicates with the lower-layer protocols and the host device (mobile phone for example). The host contains a processor, the L2CAP, which supports the upper-layer protocols and communicates between upper and lower layers. The upper-layer protocols consist of service-specific applications that must be integrated into the host application. Another element in the Bluetooth stack that relates to radio communications is the RFCOMM protocol. This protocol allows emulation of serial ports over the L2CAP. The Service Discovery Protocol (SDP) provides the means for Bluetooth applications to discover the services and the characteristics of the available services that are unique to Bluetooth. The Bluetooth device manager provides for device inquiry and connection management services.
2.4.2 Links and channels

Links and channels are used to transmit data between Bluetooth units. First, the links are established. Bluetooth technology supports two link types: synchronous connection-oriented (SCO) and asynchronous connectionless (ACL) links. The SCO links are used primarily for voice communications. The ACL links are used for packet data. Bluetooth devices can use either link type and can change link types during transmissions, although an ACL link must be established before an SCO link can be used. After the link has been established, Bluetooth uses five logical channels to transfer different types of information between devices. Control layer, physical links, logical links, LMP and L2CAP. The lowest three layers of the Bluetooth stack are sometimes grouped into a subsystem known as the control layer (RF, link controller, baseband). A physical link represents a baseband connection between Bluetooth enabled devices. A physical link is always associated with exactly one physical channel. A variety of logical links are available to support different application data transport requirements. Each logical link is associated with a logical transport, which has a number of characteristics. The Link Manager Protocol (LMP) is used to control and negotiate all aspects of the operation of the Bluetooth connection between two devices. The Bluetooth logical link control and adaptation protocol (L2CAP) supports higher level protocol multiplexing, packet segmentation and reassembly, and the conveying of quality of service information.

2.5 Security

Today’s wireless world means that data is being sent invisibly from device to device and from person to person. This data, in the form of emails, photos, contacts, addresses and more needs to be sent securely. Bluetooth wireless technology has put an emphasis on security while making connections among devices. The Bluetooth Special Interest Group has a Security Expert Group. It includes engineers from its member companies. They provide critical security information and requirements as the Bluetooth wireless specification evolves. Developers that use Bluetooth wireless technology in their products have several options for implementing security. There are three modes: non-secure, service level enforced security and link level enforced security. The manufacturer of each product determines one of these security modes. Devices and services have different security levels. For devices, there are two levels: “trusted devices” and “untrusted devices.” A trusted device has already been paired with one of your other devices, and has unrestricted access to all services.

Bluetooth technology provides fast, secure voice and data transmissions. The range for connectivity is up to 10 meters, and line of sight is not required. The Bluetooth radio unit functions even in noisy radio environments, ensuring audible voice transmissions in severe conditions. It protects data by using error-correction methods. It provides a high transmission rate and encrypts and authenticates for privacy. As with any wireless interface, Bluetooth must address issues involving reliable delivery of information. Noise and interference from other ISM (Industrial, Scientific and Medical) band transmissions, for example, are factors that come into play. To help deliver accurate information, Bluetooth provides two error-correction mechanisms: forward error correction (FEC) and automatic repeat request (ARQ). Forward error correction is applied to voice traffic for which the timeliness of the delivery takes precedence over the accuracy, because late voice traffic is unacceptable. Because Bluetooth operates in the unlicensed ISM frequency band, it competes with signals from other devices, such as garage door openers and microwave ovens. In order for Bluetooth devices to operate reliable, each Bluetooth network is synchronized to a specific frequency pattern. The Bluetooth unit moves through 1 600 different frequencies per second and the pattern is unique to each network.

There has been some confusion and misinformation surrounding security and Bluetooth wireless technology. The encryption algorithm in the Bluetooth specifications is secure. This includes not just mobile phones that use Bluetooth technology, but also devices such as mice and keyboards connecting to a PC, a mobile phone synchronizing with a PC and a PDA using a mobile phone as a modem, to name a few of the many used cases. The Bluetooth SIG works with members to investigate any issues that are reported to un-
understand the root cause of the issue. When it’s a specification error, the SIG works with members to create patches and ensure future devices don’t suffer the same vulnerability. This is an on-going process. The recently reported cases of advanced hackers gaining access to information stored on mobile phones using Bluetooth functionality are due to incorrect implementation of the Bluetooth stack by the manufacturers. The names bluesnarfing and bluebugging have been given to these methods of illegal access to information.

3. CONCLUSION

People are spending more time in the car these days and staying connected is becoming increasingly important. Bluetooth wireless devices are ideal when on the move. Keep your eyes on the road, your hands on the wheel and leave the cables at home while talking on the phone using a wireless headset or wireless speaker phone. Use a Bluetooth stereo adapter to connect your iPod or MP3 players to your Bluetooth car system and take your music with you anywhere you go. Don’t get lost with a Bluetooth enabled GPS. It will keep tabs on you and send that information to your PDA or laptop. Many of them will even double as a car kit. Get the most at your desk with a simplified wireless workspace. Today, with Bluetooth wireless technology, your office space can be clean and organized, with fewer cables in sight. Sync your PC with your mobile device to share calendars and contact lists, connect all peripherals wirelessly to communicate directly with computers. Transfer files easily from one computer to another or from your PC to the printer across the room. Also make laptop use easier with a Bluetooth enabled mouse. With Bluetooth technology at least your devices can be neat and organized, even if the rest of your office isn’t. With Bluetooth technology your music becomes a mobile collection that follows you wherever you go. Create the perfect playlist and then connect to your wireless headphones or speakers and rock out! With Bluetooth technology you can transfer photos, files, contacts and more without ever plugging in. Print photos straight from your Bluetooth enabled phone to a Bluetooth printer or transfer your favorite photos to a friend’s mobile device or laptop without ever picking up a cable. The possibilities are endless and evolving. Bluetooth technology delivers reliable wireless connectivity, with respect to interference, security and range. Bluetooth is still the best wireless implementation available for personal computing hardware everywhere.
4. Graphical Glossary

**PDA:** Personal Digital Assistants are handheld computers, but have become much more versatile over the years. PDA's have many uses: calculation, use as a clock and calendar, accessing the Internet, sending and receiving E-mails, video recording, ...

**computer peripherals:** A peripheral is a piece of computer hardware that is added to a host computer. More specifically, the term is used to describe those devices that are optional. Like a printer, scanner, ... (randapparatuur)

**Special Interest Group:** SIG is a community with a particular interest in a specific technical area. SIGs exist for the fields of computing architecture, graphics, security, etc. Members of a SIG cooperate to produce solutions within their particular field.

**piconet:** A collection of devices occupying a shared physical channel (network) where one of the devices is the piconet master and the remaining devices are connected to it (caled slaves). (een Bluetooth netwerk)

**Encryption:** is a method of encoding data to prevent others from being able to open and read the information. (codering)

**synchronizing:** refers to the idea that multiple processes are to join up or handshake at a certain point, so as to reach an agreement or commit to a certain sequence of action. Data synchronization refers to the idea of keeping multiple copies of a dataset in coherence with one another, or to maintain data integrity. (gelijkstellen)

**Interference:** is the addition of two or more waves that results in a new wave pattern. The term interference refers to the interaction of waves which are coherent with each other, either because they come from the same source or because they have the same or nearly the same frequency. (storing)

**set of commands:** A command is a directive to a computer program acting interpreter in order to perform a specific task. Most commonly a command is a directive command line interface. (verzameling opdrachtsregels)

**pairing:** The process of establishing a new relationship between two Bluetooth enabled devices. During this process a link key is exchanged (either before connection or during connecting phase). (paarvorming)

**Wireless LAN:** WLAN is a wireless local area network, which is the linking of two or more computers without using wires to create a network. (draadloos lokaal netwerk)

**Ad hoc network:** Ad hoc is a network connection method which is most often associated with wireless devices. The connection is established for the duration of one session and requires no base station. Instead, devices discover others within range to form a network for those computers. (draadloos computernetwerk zonder hoofdcomputer)

**The range:** is the distance an electromagnetic signal will reach in broadcasting or referring to the allowed values for a variable. (het bereik)

**the topology:** Network topology is the study of the arrangement of the elements of a network, especially the physical and logical interconnections between nodes. A node can be defined as a point in a network at which lines intersect a device attached to a network. (topologie)

**Protocol:** is a standard that controls the connection, communication and data transfer between two computing endpoints. In its simplest form, a protocol can be defined as the rules governing the syntax, semantics and synchronization of communication. Protocols may be implemented by hardware, software or a combination of the two. (computer-taal)
An interface: defines the communication boundary between two entities, such as a piece of software, a hardware device, or a user. It may also provide a means of translation between entities which do not speak the same language, such as between a human and a computer. The interface between a human and a computer is called a user interface. Interfaces between hardware components are physical interfaces.

Authorization: is the concept of allowing access to resources only to those permitted to use them. Authorization is a process that protects computer resources by only allowing those resources that have been granted authority to use them.

Authentication: is the process of attempting to verify the digital identity of the sender of a communication such as a request to log in.

Multiplexing of data: is a term used to refer to a process where multiple analog message signals or digital data streams are combined into one signal.

Frequency-hopping: reduces the interference from other Bluetooth devices operating on another network in the same area.

Fading: refers to the distortion that a telecommunication signal experiences over certain propagation media. In wireless systems, fading is due to multipath propagation and is sometimes referred to as multipath induced fading.

5. Non-Graphical Glossary

testimonials: getuigschrift
A written affirmation of another’s character or worth; a personal recommendation.

comprised: bestaan uit
to consist of; be composed of

clutter-free: rommel-vrij
Without confused noise; not a confused or disordered state or collection.

interoperability: samenwerkbaarheid
The ability of software and hardware to communicate on multiple machines from multiple vendors.

manufacturer: fabrikant
A person, group, or company that owns or runs a manufacturing plant.

susceptible: plotselinge
accessible or especially liable or subject to some influence

attenuates: verzachten, verdunnen
To reduce in force, value, amount or degree; weaken.

interchangeable: vervangbaar, verwisselbaar
Capable of being put or used in the place of each other.

implementation: uitvoering, uitrusting
the act of accomplishing some aim; to provide with; to provide with implements

appendix: bijlagen, aanhangsel
Supplementary material at the end of a book, article, document, or other text, usually of an explanatory, statistical, or bibliographic nature.
a broad range: breed spectrum, groot bereik
not limited or narrow, large distance of reach

likelihood: waarschijnlijkheid
a probability or chance of something

intervention: tussenkomst
the act or fact of intervening; interference of one in the affairs of another

subsequent: daarop volgend, later
occurring or coming later or after; subsequent events

verified: het is bewezen
To act as ultimate proof or evidence of; serve to confirm.

sufficient: voldoende, genoeg
adequate for the purpose; enough

profound: gegrond, grondig
Being or going far beneath what is superficial, external, or obvious.

capabilities: vermogen, bekwaamheid
The ability to undergo or be affected by a given treatment or action.

convergence: samensmelting
The occurrence of two or more things coming together.

the claimant: de eiser
A person who makes a claim: a request or demand for payment in accordance with an insurance policy.

6. References


Microsoft Corporation; www.microsoft.com; “Bluetooth and Microsoft products”; june 2005

HP; www.hp.com; “Understanding Bluetooth”; january 2006

Bluetooth SIG press release; “Bluetooth® wireless technology enhances school and work experience”, september 2006

Max Brugger; Oregon State University; “The importance of being Bluetooth”; november 2006

Bluetooth SIG press release; ”The latest in Bluetooth wireless technology takes the floor at the unplugfest”, october 2007

Scientific American; Ask the experts; “How does Bluetooth work?”; november 2007