Bluetooth Network

SAGHAR KHADEM
MUHAMMAD AJMAL
FREDRIK LARSSON
SHAHAM SHARIFIAN

SSY145 WIRELESS NETWORKS
CHALMERS UNIVERSITY OF TECHNOLOGY **May 6, 2009**

Contents

Review question

What is the main difference between centrally controlled WLAN and Bluetooth network?

Introduction

Our project is about Bluetooth networks. Bluetooth was developed by SIG (Special Interest Group). The name refers to Danish king whose name was Harald Blåtand (940-981 A.D.). He unified Denmark and Norway. Bluetooth was supposed to unify telecom and computing industries and to replace cables. It is an open wireless protocol for exchanging data over a short distance. We will discuss the concept of piconet and scatternet in detail as well as Bluetooth Ad-hoc Networks and Personal Area networks (PANs).

The technology was born in 1994 by Jaap Haartsen and Sven Mattisson, who were working for Ericsson Mobile Platforms in Lund, Sweden. In 1998 The Bluetooth SIG was formed. The current promoter members of SIG are Ericsson, Lenovo, Intel, Microsoft, Motorola, Nokia, and Toshiba. Today SIG has over 11,000 members worldwide. In 1999 the first version of Bluetooth was released.

The motivation for the Bluetooth is mainly replacing cables for short-range connection between mobile devices like notebook, cellular handsets, network access points, printers, PDA's, desktops, keyboards, joysticks and mice. It also gives the ability to use a wireless headset to a cell phone, which eliminates the problems with the constantly tangled wires. Cell phones nowadays have the ability to take photographs as well as to send and receive mail and other files. If the cell phones have a Bluetooth connection it can print photos and files on a Bluetooth-equipped printer without having to connect to it via cable. It can also be used to synchronize address books and calendars between two devices.
The other important motivations can be considered as below:

- Low cost
- Low power consumption
- Small size of the chip
- Using the free ISM band
- Enough bandwidth for simultaneous voice and data support
- Simultaneous connection to multiple devices
- Devices can connect to each other without user interaction

We also aim to describe the Bluetooth networking and architecture. In Bluetooth each node is willing to forward data for other nodes, and so the determination of which nodes forward data is made dynamically based on the network connectivity. So, we investigate how nodes are connected to the network, how they manage to send packets to each other, and how these procedures are done.
Finally we go through the security in Bluetooth which is an important issue in wireless networks nowadays. The security in Bluetooth network is based on symmetric key cryptographic mechanism for authentication, link encryption, and key generation.

Networking

Piconet and Scatternet

The Bluetooth network provides two different connection types, point-to-point connection and point-to-multipoint connection. A Bluetooth network works in a master-slave like fashion. The master is the device that initializes the connection and can communicate with up to seven other devices.
The master node is in charge of setting up the communication and deciding the queue of frequency hopping and network synchronizing. This ad-hoc network group which is up to eight devices and uses the same frequency hopping channel and clock is called piconet. In each piconet the devices can switch roles so that the slave can be the master and vice versa. The roles are changed in a round-robin fashion. There can also be up to 255 inactive or parked devices that the master can bring them into active status at any time.
We have three kinds of addresses in a Bluetooth network.

1. Device address: All Bluetooth devices have a unique 48-bit address.
2. Active member address (AMA): The active slave members are assigned a 3-bits AMA
3. Parked member address (PMA): The parked members are assigned a 8-bits PMA

The Bluetooth specification allows connecting two or more piconets together. If multiple piconets are linked together they form a scatternet (see Figure 1). In this case the nodes that interconnect two piconets are considered as bridges. The bridges can be slaves in both piconet or they may be a master in one piconet and slave in another, but they cannot be master in both piconets. The bridges share their active time between the piconets that they are connected to.

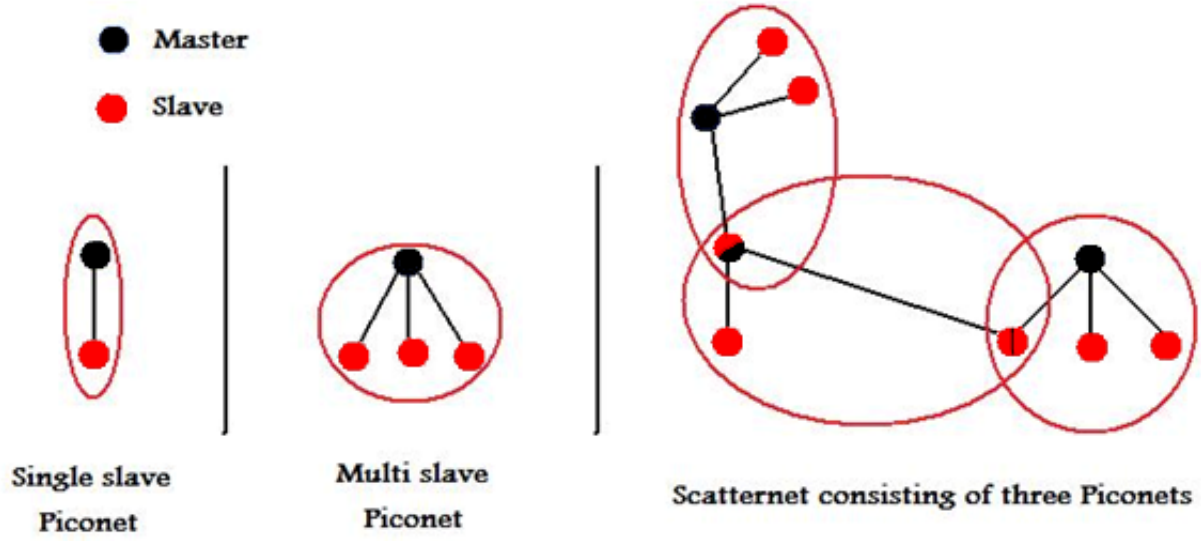

Figure 1: Piconet and Scatternet

Master/Slave switch

Bluetooth transceiver uses time-division duplex (TDD). It means that the master initiates the connection at even time slots, and the slave starts transmitting at odd time slots. The master clock synchronizes the piconet, and it never adjusts its system clock during the existence of piconet. The slaves adopt their clock with the master clock. This updating is done every time a packet is received from the master.

If a slave wants to become a master, a master-slave switch needs to take place. The switch takes place in two steps: first there is a reversal of the TDD scheme between the two considered devices. Second, because the piconet parameters are based on the address and clock of the master, a piconet switch must be performed by all the nodes in the piconet.

Functional Overview

Each device in a Bluetooth network can have 8 functional modes which are shown in Fig 2. We describe each of them here:

- **Standby:** The device is in standby mode when there is no connection, but it waits for incoming messages.
- **Inquiry:** This message is transmitted to find all public devices in its range when other device addresses are not known. After inquiry the page message is transmitted
- **Page:** A connection is initiated with a page message when the device address is known. After receiving a response from devices, the master assigns AMA to each device and the slaves synchronize to the master.
- **Connected:** In the connect state, the slave just waits for the master to poll it.
- **Transmit:** In the transmit state, the slave can transmit the data when the master polls it.
- **Park:** When a device is in park state, it receives a PMA and the AMA is given up, but the device is still synchronized by listening to the broadcasting messages, and does not transmit data.
- **Hold:** When a device is in hold state, it is inactive in a predetermined amount of time. The AMA is retained.
- **Sniff:** When a device is in sniff state, it is inactive in a predetermined amount of time, and then wakes up to do data transmission and then goes to sleep again. The AMA is retained.

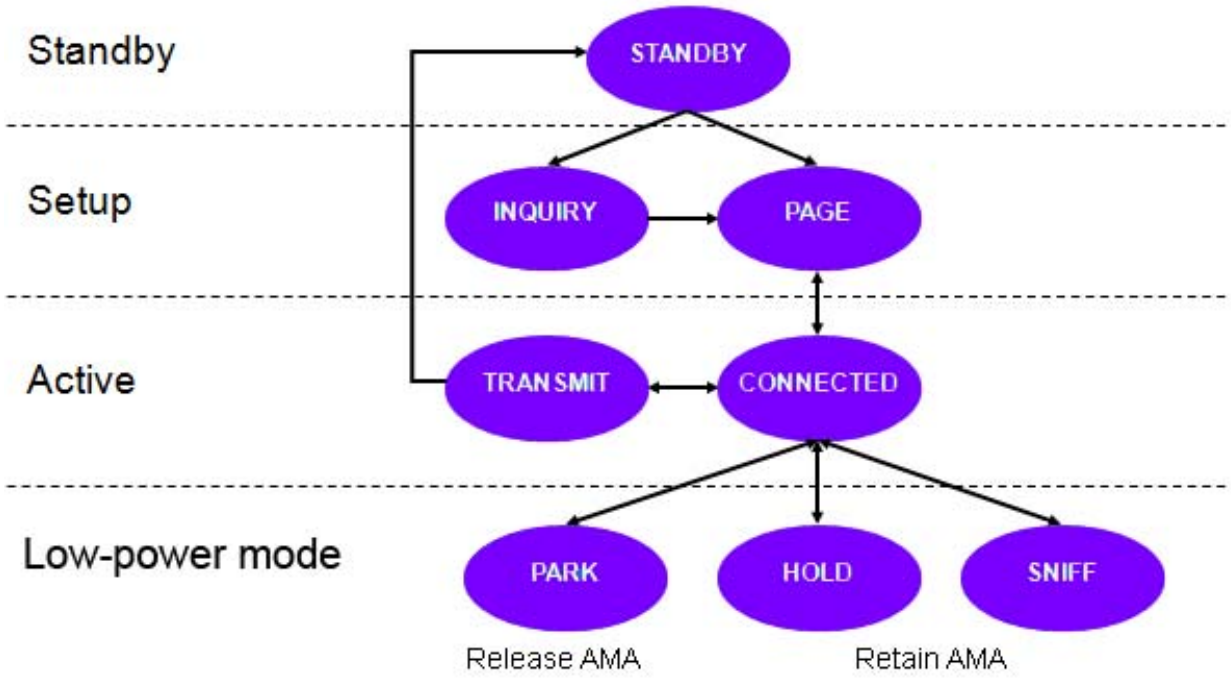

Figure 2: Functional overview

Comparison between centrally controlled wireless LANs and Bluetooth networks

Centrally controlled WLAN is a fixed network infrastructure which uses access points. An access point communicates with devices in wireless network. Access point devices typically have coverage areas up to 100 meters (802.11g) which is called a cell or range. Users move freely within the cells by linking the access points together. The data rate in WLANs (802.11g) can be up to 128 Mbps. The new version of WLAN is 802.11n. It is supposed to be released in January 2010 which has a range up to 300 meters and the data rate up to 600 Mbps.

Ad hoc networks can dynamically connect remote devices. For example Bluetooth networks are considered as ad hoc networks because of their shifting network topologies. Since it is an ad hoc network it can cover an area as large as 10 meters in range in the normal case but the range can be extended up to 100 meters. The flow of data is done by access points in WLANs, but in Bluetooth networks this is done by master nodes. The data rate of Bluetooth 2.1 is up to 3 Mbps, but with the new release of Bluetooth 3.0 it can reach up to 24 Mbps.

Frequency hopping spread spectrum (FHSS)

The FHSS is a technique that trades bandwidth efficiency for more reliability, integrity, and security. It reduces the interference of other devices using the same channel. It chops the total bandwidth up to 79 different channels. The devices hop through these channels every 625 microseconds. Since the ISM band is used in Bluetooth the interference can be from many devices such as baby monitors, microwave ovens and cordless phones. Each channel has the bandwidth of 1 MHz and the master node decides how the hopping should be done.

Physical link types

Two kinds of links can be established between the master and the slave(s):

- Synchronous Connection-Oriented (SCO) link
- Asynchronous Connection-Less (ACL) link

SCO link is a point-to-point link between the master and a specific slave. There are reserved time slots in SCO link which are used to send data packets. The packets are never retransmitted. It supports time-critical information such as voice, conversation. Three SCO links can be supported by master to same or different slaves. And also a slave can support up to a maximum of 3 SCO links from the same master and otherwise two. SCO links have a data rate up to three parallel channels of 64Kbps each. The bandwidth for these links is guaranteed.

ACL link is a point-to-multipoint link. The slots that are not reserved for SCO can be used by ACL. To ensure the integrity, retransmission is done in ACL. In ACL the packet switch connection is used between the master and all active slaves. The packets with no address are considered as a broadcast packet which is sent to every slave. ACL links have a data rate up to 1 Mbps.

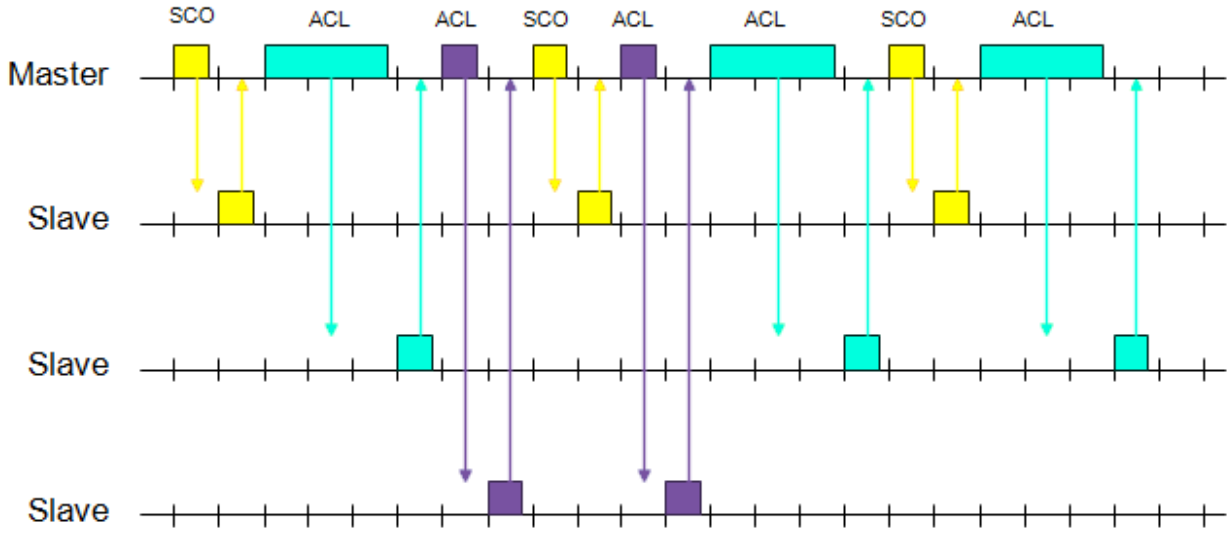

Figure 3: Example of a TDD scheme

Security

Three basic security services are implemented in Bluetooth networking:

- **Authentication:** This service verifies the identity of communication devices. If the device cannot authenticate properly the connection is aborted.
- **Confidentiality:** This service prevents the passive attacks such as eavesdropping by only allowing authorized devices.
- **Authorization:** This service specifies which devices are authorized to access different services.

Different modes of security

Bluetooth has three different kinds of security modes. Devices can only operate in one mode at a specific time.

- **Security mode 1:** Non-secure mode
- **Security mode 2:** Service-level enforced security mode
- **Security mode 3:** Link-level enforced security mode

Actually in security mode 1 there is no security. It allows other Bluetooth devices to connect without implementing any security. Some applications do not require security such as exchanging business cards.

In security mode 2 security procedures are initiated after channel establishment. The centralized security manager keeps policies for access control and interface with other protocols and devices. Here it is possible to give access to some services without giving access to other services. This is a service level

security which is very flexible based on policy, thus authentication, confidentiality and authorization can be provided.

In security mode 3, the security procedure is initiated by the Bluetooth device during the channel establishment. This mode supports authentication and confidentiality by using a secret link key for encrypting data. This key (the pairing procedure) is generated when two devices communicate for the first time. This is done during the initialization phase when the users enter identical PIN codes into both devices. The PIN codes can vary between 1 and 16 bytes. Since security mode 3 is a fixed link level security, it can just provide authentication and confidentiality.

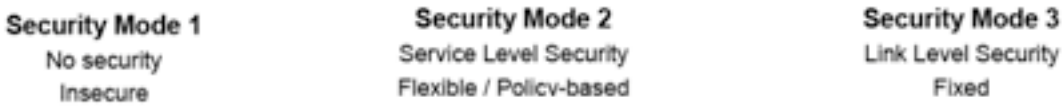

Figure 4: The different security modes

Because Bluetooth only provides link authentication and link encryption, there cannot be end-to-end security. This problem is solved by providing higher layer security on top of Bluetooth.

Authentication

Authentication procedure is in the form of a "challenge-response" scheme between a claimant device and a verifier device. User authentication is not provided. The protocol uses the knowledge of the secret key to validate the claimant device. If the authentication fails the Bluetooth device will wait a certain time interval before a new attempt is done. This time interval increases exponentially to avoid trial-and-error with different keys. This protocol does not protect against sophisticated attacks such as offline searching, and man-in-the-middle attacks due to the simple one-way-only challenge-response authentication.

Confidentiality

Stream cipher is used in the Bluetooth encryption procedure. We have three different encryption modes:

- **Encryption mode 1:** No encryption is done in this mode.
- **Encryption mode 2:** This mode does not give encryption to broadcast traffic, but it gives encryption to point-to-point traffic.
- **Encryption mode 3:** All traffic is encrypted by using the master link key, which is shared by every device.

Authorization

Bluetooth devices can be either trusted or un-trusted. Trusted devices have full access to all services, and have a fixed relationship. Un-trusted devices have limited service access because they don't have a permanent relationship. Bluetooth has three levels of security to deal with un-trusted devices. These levels are described as follows:

- **Service level 1:** Trusted devices have automatic access to all services, but for un-trusted devices, user-assisted authorization is needed to access services.
- **Service level 2:** Devices only need to be authenticated to gain access to all services.
- **Service level 3:** This service is open to every device. Devices gain access automatically without the need of authentication.

Progression timeline of Bluetooth

Bluetooth 1.0 and 1.0B

It was released on May 20, 1998. This version had lots of problems, and the manufacturers had difficulties to get their devices work together. All devices were required to have a mandatory device address. This was a problem for some certain services that required anonymity.

Bluetooth 1.1

It was released on February 22, 2001. This was the first successful version of Bluetooth. It fixed a lot of problems that exist in the previous version, which gave better interoperability. This version also gave support to non-encrypted channels.

Bluetooth 1.2

It was released on November 5, 2003. This version is backwards compatible with the previous version. It gave faster connection and discovery. It was equipped with adaptive frequency-hopping spread spectrum (AFH) which reduced interference by avoiding crowded frequencies in the hop sequence. The transmission speed was increased up to 721 kbps. It has improved voice quality of audio links by allowing retransmission of corrupted packets. It also provides better support for concurrent data transfer. RSSI is included. RSSI is an indication of the power level being received by the antenna. If the ISSR is higher the signal is stronger.

Bluetooth 2.0

It was released on November 10, 2004. The main improvement in this version is the enhanced data rate (EDR) which gave this version three times faster transmission speed up to 2.1 Mbps. Different radio technology were used to improve data transmission. It also had lower power consumption by reducing the duty cycle. It allows the connection of multiple devices without the lag factor which was a problem in Bluetooth 1.2.

Bluetooth 2.1

It was released on July 26, 2007. The main changes in this version are as follows:

- **Secure simple pairing:** The security is improved in many ways. One of these is by generating a six-digit passkey. The user enters the passkey to authenticate both devices. This passkey differs from a PIN code. The initiating device generates this for every connection sequence which is unique to each connection.

- **Near field communication (NFC) cooperation:** This is a part of secure simple pairing. This feature creates a secure connection by just bringing the devices close to each other.
- **Sniff subrating:** This feature introduces the SNIFF low power mode.
- **Encryption pause resume:** This gives an option to refresh encryption keys, results in stronger encryption for connections longer than a Bluetooth day (23.3 hours).
- **Extended inquiry response:** This provides more information about the devices such as the name of the device, a list of services the device supports, and the time of day. This allows a better filtering of devices before connection.

Bluetooth 3.0

It was released on April 21st, 2009. This version introduces the AMP (Alternate MAC/PHY) and Wi-Fi as a high speed transport. The biggest change in Bluetooth 3.0 is its high speed which is borrowed from Wi-Fi. It boosts the throughput up to 24 Mbps. It can be used to create an ad hoc network connection (802.11) between devices.

- **Alternate MAC/PHY:** When users want to transfer lot of data it can change to Wi-Fi instead of using the usual Bluetooth radio. This gives lower power per bit to transfer data than using the previous method.
- **Unicast connectionless data:** For small amount of data this gives a lower latency between user action and reconnection/transmission of data.

Future development

On April 2009 SIG presented a new low power Bluetooth which had a new protocol stack which was compatible with the other protocol stacks. It is called Bluetooth low energy. This technology can be expected to be used by watches displaying caller ID information, sports sensors monitoring your heart rate during exercise, and medical devices. Devices using this technology have the possibility to have a battery life up to one year.

The developers of UWB, WiMedia, have announced it will transfer all current and future specifications to SIG. This means that UWB and Bluetooth will be merged together. This will result in future high speed and power optimized implementations.

There are also plans to improve the QoS in Bluetooth, enabling transmission of audio and video data at a high quality.

Conclusion

Bluetooth was first an unsecure technology for making personal area networks, and the main goal of it was to replace cables. It has evolved from a very simple technology into a more useful technology, supporting a family of devices capable of high performance in many different areas. With the emerging of the different versions of Bluetooth the security and throughput were the main things that were improved. Bluetooth network is an ad hoc network because it was meant to let devices to connect to each other under varying network topologies. With the new version in Bluetooth (V 3.0) there was a great increase in data rate which make Bluetooth a very versatile technology.

For further information you can view the reference list. In order to gain full in-depth overview of Bluetooth you should study the protocol stack which was not done in this report.

Reference list

[1] Christian Gehrmann & Joakim Persson &Ben Smeets, 2004, Bluetooth Security, ARTECH HOUSE inc, Norwood, MA 02062

[2] Li Dao-Hui, Lin Gang, Gao Bao-Xin, 2002, The Radio Networking of Bluetooth, 3rd International Conference of Microwave and Millimeter wave Technology Proceedings, Beijing, China, 24 April 2009, <http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=01187676>

[3] Tom Karygiannis, Les Owens, 2002, "Wireless Network Security 802.11 Bluetooth and Handheld Devices", 1st edition, the National Institute of Standards and Technology (NIST), Gaithersburg, Maryland, US, viewed 24 April 2009, <http://csrc.nist.gov/publications/nistpubs/800-48/NIST_SP_800-48.pdf>

[4] SIG 2009, SIG, Bellevue, Washington, USA, viewed 24 April 2009, <www.bluetooth.com>

[5] Bluetooth Wiki 2009, Bluetooth, wiki article, 22 April, viewed 24 April 2009, < http://en.wikipedia.org/wiki/Bluetooth>.

[6] Oryl, Michael 2009, New Bluetooth 3.0 supports 802.11b/g connections, new "Low Energy" spec coming later this year, MobileBurn.com, viewed 1 May 2009, <http://www.mobileburn.com/news.jsp?Id=6875>

[7] Ranganath Duggirala, Roy L. Ashok and Dharma P. Agrawal, 2003, Energy Efficient Bridge Management Policies for Inter-Piconet Communication in Bluetooth Scatternets, University of Cincinnati – Cincinnati, Ohio, 1 May 2009, <http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=01285086>

[8] McDermott-Wells, Patricia, 2004, What is Bluetooth?, IEEE potentials, Vol. 23, No. 5, 1 May 2009, <http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=01368913>