http://developers.sun.com/techtopics/mobility/midp/articles/bluetooth1/ Dec 19, 2004

Article

Wireless Application Programming with J2ME and Bluetooth

by Qusay H. Mahmoud
February 2003

Electronic devices connect to one another in a variety of ways: A cable connects a computer's processing unit to a display, a data cable and a docking cradle connect a personal digital assistant (PDA) or a cellular phone to a computer, radio waves connect a cordless phone to its base unit, an infrared beam connects a remote control to a television. The elaborate array of connectors among electronic devices cries out for a better solution. That's where Bluetooth comes in.

Bluetooth is a completely different way to form connections between electronic devices in close proximity. You can think of it as *a cable-replacement technology*, but its applications are limited only by our imaginations. Bluetooth does more than just replace cables. It is a radio-frequency technology that uses the 2.4 GHz Industrial-Scientific-Medical (ISM) band. If you have a baby monitor or a garage-door opener you're already using the ISM band.

This two-part series of articles will show you how to use J2ME and Bluetooth to develop next-generation wireless applications for tomorrow's market. This first article covers the basics of Bluetooth; the next one will concentrate on using the Java APIs for Bluetooth Wireless Technology (JSR 82) to develop Java technology-enabled applications for Bluetooth-enabled devices. This article starts by presenting a brief overview of the technology, then explains:

- The differences between Bluetooth and two similar technologies, infrared and 802.11b
- Features and future applications
- The architecture of Bluetooth and its protocol stack
- Network topologies
- Procedures for establishing connections
- The role of profiles
- Security considerations
- Products now on the market

Overview of Bluetooth

The Bluetooth wireless connectivity technology was originally envisioned in 1994 by the Swedish phone equipment maker Ericsson as a way for mobile devices to communicate with each other at short ranges -- up to 30 feet, or 10 meters. In 1998, Ericsson, IBM, Intel, Nokia, and Toshiba formed the Bluetooth Special Interest Group consortium to develop a royalty-free, open specification for short-range wireless connectivity. Since then, more than 2000 companies have joined the Bluetooth SIG, including virtually all manufacturers of phone, computer, and PDA equipment.

While Bluetooth is positioned as a replacement for cable, infrared, and other connection media, it offers a variety of other services, and creates opportunities for new usage models. For instance, it's also a good technology for synchronizing devices. It works quietly, unconsciously, and automatically in the background.

"Bluetooth" was the nickname of Harald Blåtland II, king of Denmark from 940 to 981, who united all of Denmark and part of Norway under his rule. A runic stone has been erected in his capital city, Jelling. The runes say:

```
Harald Christianized the Danes
Harald controlled Denmark and Norway
Harald thinks notebooks and cellular phones should communicate seamlessly
```

Bluetooth vs. Infrared

Home electronics devices like TVs and VCRs communicate using beams of light in the infrared spectrum. Infrared is fairly reliable and doesn't cost much to build into devices. It does have drawbacks:

- It's line-of-sight, so a sender must align with its receiver.
- It's one-to-one, so a device can't send to multiple receivers at the same time.

Infrared's advantages are consequences of its disadvantages:

- Because it's line-of-sight, interference is uncommon.
- Because it's one-to-one, message delivery is reliable: each message sent goes to the intended recipient no matter how many infrared receivers are in the room.

Bluetooth vs. 802.11b

While both Bluetooth and IEEE 802.11b are wireless communication protocols and both operate in the 2.4GHz band, it is important not to visualize Bluetooth as a replacement for 802.11 wireless LAN technology. They're designed to accomplish different goals.

The 802.11b protocol is designed to connect relatively large devices with lots of power and speed, such as desktops and laptops. Devices communicate at up to 11 Mbit/sec, at greater distances (up to 300 feet, or 100 meters). By contrast, Bluetooth is designed to connect small devices like PDAs, mobile phones, and peripherals at slower speeds (1 Mbit/sec), within a shorter range (30 feet, or 10 meters), which reduces power requirements.

Note: Common terminology is suggestive. Those familiar with both say that IEEE 802.11b connects devices in a wireless local area network (LAN), while Bluetooth connects devices in a Personal Area Network (PAN).

Another major difference is that 802.11b wasn't designed for voice communications, while any Bluetooth connection can support both data and voice communications.

Note: The IEEE has designated its version of the Bluetooth specification 802.15. This version will complement 802.11b technology, and boost Bluetooth's transmission speed to 20 Mbit/sec, which would, for example, make it feasible to download photos from a digital camera wirelessly.

Several web sites compare Bluetooth and 802.11b point by point, and many of these stress that the two are complementary rather than competitive. For dozens of related links, visit Bluetooth and (not Versus) Wi-Fi (802.11).

Bluetooth Features

The major features of Bluetooth are:

- Bluetooth is wireless and automatic. You don't have to keep track of cables, connectors, and connections, and you don't need to do anything special to initiate communications. Devices find each other automatically and start conversing without user input, expect where authentication is required; for example, users must log in to use their email accounts.
- Bluetooth is inexpensive. Market analysts peg the cost to incorporate Bluetooth technology into a PDA, cell phone, or other product at around $20 now, and say that it could fall to as little as $5 per unit.
- The ISM band that Bluetooth uses is regulated, but unlicensed. Governments have converged on a single standard, so it's possible to use the same devices virtually wherever you travel, and you don't need to obtain legal permission in advance to begin using the technology.
- Bluetooth handles both data and voice. Its ability to handle both kinds of transmissions simultaneously makes possible such innovations as a mobile hands-free headset for voice with applications that print to fax, and that synchronize the address books on your PDA, your laptop, and your cell phone.
- Signals are omni-directional and can pass through walls and briefcases. Communicating devices don't need to be aligned and don't need an unobstructed line of sight.
- Bluetooth uses *frequency hopping*. Its *spread spectrum* approach greatly reduces the risk that communications will be intercepted.

Bluetooth Applications

Bluetooth wireless technology can be used for these applications:

- File transfer.
- Ad-hoc networking: Communicating devices can spontaneously form a community of networks that persists only as long as it's needed
- Device synchronization: Seamless connectivity among PDAs, computers, and mobile phones allows applications to update information on multiple devices automatically when data on any one device changes.
- Peripheral connectivity.
- Car kits:Hands-free packages enable users to access phones and other devices without taking their hands off the steering wheel
- Mobile payments: Your Bluetooth-enabled phone can communicate with a Bluetooth-enabled vending machine to buy a can of Diet Pepsi, and put the charge on your phone bill.

Bluetooth Network Topology

Bluetooth-enabled devices are organized in groups called *piconets*. A piconet consists of a master and up to seven active slaves. A master and a single slave use point-to-point communication; if there are multiple slaves, point-to-multipoint communication is used. A master unit is the device that initiates the communication. A device in one piconet can communicate to another device in another piconet, forming a *scatternet*, as depicted in Figure 1. Notice that a master in one piconet may be a slave in another piconet:

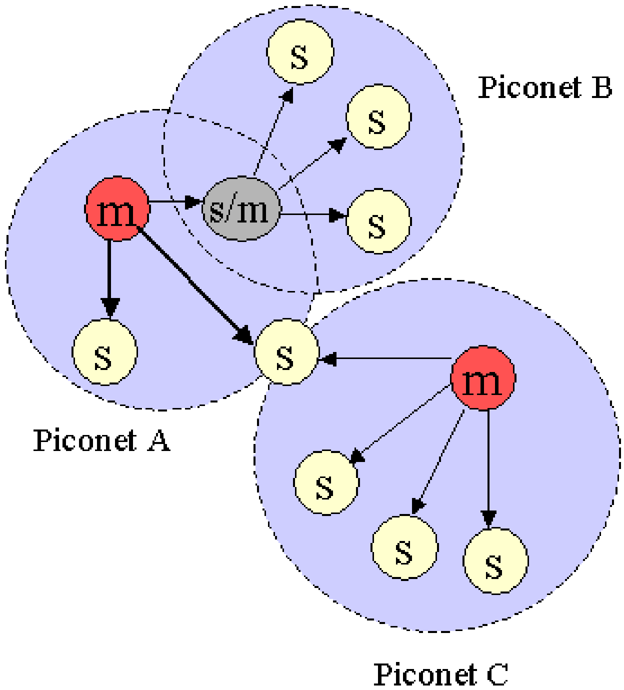

Figure 1: Scatternet Comprising Three Piconets

The normal duration of transmission is one slot, and a packet can last up to five time slots in length. In order to support full-duplex communications, Bluetooth uses a time-division multiplexing (TDM) scheme, in which a master device always uses an even-numbered slot when it transmits, and a slave uses an odd-numbered slot.

Low-Power Operating Modes

Bluetooth defines provisions for three low-power operating modes in order to conserve battery life:

- In *sniff* mode, a slave listens at a reduced level and doesn't take an active role in the piconet.
- A device in *hold* mode transmits no data, but its clock continues to operate, and a slave remains in synchronization with the master. The device is not an active member of the piconet, but it retains its active member address. Power requirements decrease as a device goes from sniff to hold.
- *Park* mode is like hold mode in that the slave is synchronized to the master but is not part of the traffic. In this mode, however, the slave doesn't retain its active member address. Power requirements decrease still further as a device goes from hold to park.

The Bluetooth Protocol Stack

The Bluetooth specification is over 1500 pages long and contains the information necessary to ensure that diverse devices supporting this technology can communicate with each other worldwide. The specification is divided into two sections: Core Specification (Volume I) and Profile Definitions (Volume 2).

Here's a high-level view of the architecture of the Bluetooth protocol stack:

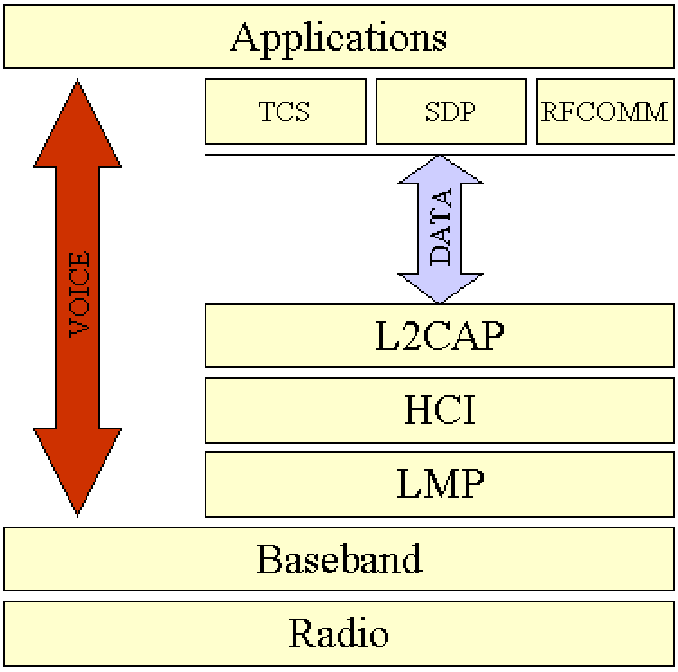

Figure 2: Bluetooth Protocol Stack

The responsibilities of the layers in this stack are as follows:

- *The radio layer* is the physical wireless connection. To avoid interference with other devices that communicate in the ISM band, the modulation is based on fast frequency hopping. Bluetooth divides the 2.4 GHz frequency band into 79 channels 1 MHz apart (from 2.402 to 2.480 GHz), and uses this spread spectrum to hop from one channel to another, up to 1600 times a second. The standard wavelength range is 10 cm to 10 m, and can be extended to 100 m by increasing transmission power.
- *The baseband layer* is responsible for controlling and sending data packets over the radio link. It provides transmission channels for both data and voice. The baseband layer maintains Synchronous Connection-Oriented (SCO) links for voice and Asynchronous Connectionless (ACL) links for data. SCO packets are never retransmitted but ACL packets are, to ensure data integrity.

  SCO links are point-to-point symmetric connections, where time slots are reserved to guarantee timely transmission. A slave device is allowed to respond during the time slot immediately following an SCO transmission from the master. A master can support up to three SCO links to a single slave or to multiple slaves, and a single slave can support up to two SCO links to different slaves.

  Data transmissions on ACL links, on the other hand, are established on a per-slot basis (using slots not reserved for SCO links). ACL links support point-to-multipoint transmissions. After an ACL transmission from the master, only a slave addressed specifically may respond during the next time slot; if no device is addressed, the message is treated as a broadcast.
- *The Link Manager Protocol (LMP)* uses the links set up by the baseband to establish connections and manage piconets. Responsibilities of the LMP also include authentication and security services, and monitoring of service quality.
- *The Host Controller Interface (HCI)* is the dividing line between software and hardware. The L2CAP and layers above it are currently implemented in software, and the LMP and lower layers are in hardware. The HCI is the driver interface for the physical bus that connects these two components. The HCI may not be required. The L2CAP may be accessed directly by the application, or through certain support protocols provided to ease the burden on application programmers.
- *The Logical Link Control and Adaptation Protocol (L2CAP)* receives application data and adapts it to the Bluetooth format. Quality of Service (QoS) parameters are exchanged at this layer.

Establishing a Network Connection

When a device is not connected to a piconet, it is in a standby mode. In this mode, the device listens for messages every 1.28 seconds over 32 hop frequencies. When one device wishes to establish a connection with another, it sends out 16 identical *page* messages on 16 hop frequencies. If the slave doesn't respond, the master retransmits the page message on the other 16 hop frequencies. If the master doesn't know the slave's address it must precede the page message with an *inquiry* message, which requires an extra response from the slave unit. When the slave responds to the page message, the master can begin transmitting voice or data.

To understand how Bluetooth-enabled devices establish network connections, let's assume that Sally wishes to access her e-mail messages from her Bluetooth-enabled device as she enters a hotel or a mall. Once Sally taps the email application icon, the following procedures are carried out automatically:

1. *Inquire*: In a new environment, the device automatically initiates an inquiry to find an access point. All nearby access points respond with their addresses, and the device picks one.
2. *Page*: The paging procedure synchronizes the device with the access point.
3. *Establish a link*: The Link Manager Protocol establishes a link with the access point.

4. *Discover services*: The LMP uses the Service Discovery Protocol (SDP) to find out what services are available from the access point. Here we assume that the email service is available.
5. *Create an L2CAP Channel*: The LMP uses information obtained from the Service Discovery Protocol (SDP) to create an L2CAP channel to the access point. The application may use this channel directly or use a protocol like RFCOMM (Radio Frequency Communications Protocol) that might be running over L2CAP. RFCOMM emulates a serial line.
6. *Create an RFCOMM channel*: Depending on the needs of the application, an RFCOMM channel (or another channel) is created over the L2CAP channel. Creating an RFCOMM channel allows an existing application that works with serial ports to work with Bluetooth as well, without any modifications.
7. *Authenticate*: This is the only step that requires input from the user. If the access point requires authentication, it will send an authentication request, and the user will be prompted to enter a PIN to access the service. For security reasons, the PIN code itself is not sent over the wireless link, but rather a key generated from it.
8. *Log in*: If the devices use the Point-to-Point Protocol (PPP) over RFCOMM, a serial port is emulated, and Sally can log in to her email account.
9. *Send and receive data*: The email client and the access point now use standard network protocols like TCP/IP to send and receive data.

Bluetooth Profiles

Bluetooth profiles are intended to ensure interoperability among Bluetooth-enabled devices and applications from different manufacturers and vendors. A profile defines the roles and capabilities for specific types of applications. Note well that Bluetooth devices cannot interact unless they conform to a particular profile -- having the bare minimum Bluetooth stack isn't enough.

All of the Bluetooth profiles are defined in Volume II of the Bluetooth specification. Here are some of them:

- The *Generic Access Profile* defines connection procedures, device discovery, and link management. It also defines procedures related to use of different security models and common format requirements for parameters accessible on the user interface level. At a minimum all Bluetooth devices must support this profile.
- The *Service Discovery Application and Profile* defines the features and procedures for an application in a Bluetooth device to discover services registered in other Bluetooth devices, and retrieves information related to the services.
- The *Serial Port Profile* defines the requirements for Bluetooth devices that need to set up connections that emulate serial cables and use the RFCOMM protocol.
- The *LAN Access Profile* defines how Bluetooth devices can access the services of a LAN using PPP, and shows how PPP mechanisms can be used to form a network consisting of Bluetooth devices.
- The *Synchronization Profile* defines the application requirements for Bluetooth devices that need to synchronize data on two or more devices.

Bluetooth Security

Security is provided in three ways: pseudo-random frequency hopping, authentication, and encryption. Frequency hops make it difficult for anyone to eavesdrop. Authentication allows a user to limit connectivity to specified devices. Encryption uses secret keys to make data intelligible only to authorized parties.

All Bluetooth-enabled devices must implement the Generic Access Profile, which contains all the Bluetooth protocols and possible devices. This profile defines a security model that includes three security modes:

1. *Mode 1* is an insecure mode of operation. No security procedures are initiated.
2. *Mode 2* is known as *service-level enforced security*. When devices operate in this mode, no security procedures are initiated before the channel is established. This mode enables applications to have different access policies and run them in parallel.
3. *Mode 3* is known as *link-level enforced security*. In this mode, security procedures are initiated before link setup is complete.

Note: The authentication method built into Bluetooth authenticates the device and not the device's user or owner, so the user must consider the use of an application-layer security program and take care that the device itself doesn't fall into the hands of a third party.

Bluetooth Products on the Market

Since the inception of Bluetooth technology, companies that have adopted it have been developing products for it. Bluetooth products on the market today range from PC cards available from IBM and Toshiba to a hands-free car kit. Like 802.11b wireless LAN cards, the PC cards slide into a PCMCIA slot on a laptop but, while 802.11b wireless cards connect a computer wirelessly to a LAN, Bluetooth cards connect a device to other Bluetooth-enabled devices. More than 800 qualified Bluetooth-enabled devices and accessories are available at this writing.

Conclusion

This article presented the basics of Bluetooth, a radio-frequency technology that uses the Industrial-Scientific-Medical band at 2.4 GHz. You learned about the technology's attractions, including the low cost to incorporate it into electronic devices. The Bluetooth protocol stack was presented and the procedures for establishing a connection between Bluetooth devices were described. Stay tuned for the second article in this series, which will cover the Java APIs for Bluetooth Wireless Technology.

For more information

- Bluetooth Specifications
- Bluetooth and (not Versus) Wi-Fi (802.11)
- Bluetooth SIG, Inc. (Member Website)
- Bluetooth Qualification Process
- Bluetooth Qualified Products

Acknowledgments

Special thanks to Teck Yang Lee of Sun Microsystems whose feedback helped me improve the article.

About the Author: Qusay H. Mahmoud provides Java consulting and training services. He has published dozens of articles on Java, and is the author of *Distributed Programming with Java* (Manning Publications, 1999) and *Learning Wireless Java* (O'Reilly & Associates, 2002).

Reader Feedback

Excellent **Good** **Fair** **Poor**

If you have other comments or ideas for future technical tips, please type them here:

Comments:

If you would like a reply to your comment, please submit your email address:

Note: We may not respond to all submitted comments.

Submit »

Have a question about Java programming? Use Java Online Support.

Back To Top