Understanding Bluetooth™

January 2002

Executive Summary

Bluetooth™ wireless technology is finally here. Originally conceived as a low-power short-range radio technology designed to replace cables for interconnecting devices such as printers, keyboards, and mice, its perceived potential has evolved into far more sophisticated usage models. The requirement to do this in a totally automated, seamless, and user-friendly fashion, without adding appreciable cost, weight, or power drain to the associated host is an enormous engineering challenge.

Bluetooth devices can form piconets of up to seven slaves and one master, enabling discovery of services and subsequent implementation of many varied usage models including wireless headsets, Internet bridges, and wireless operations such as file exchange, data synchronization, and printing.

Despite talk of Bluetooth competing with wireless LANs, Bluetooth products work over shorter distances and are designed to solve different problems.

The Bluetooth SIG publishes the Bluetooth specification. The IEEE has formed the 802.15 working group to define standards for wireless PANs. The 802.15.1 standard for WPAN™s will be modeled after the Bluetooth specification from the Bluetooth SIG. Microsoft® has announced support for Bluetooth in the next release of Windows® XP.

The waters of Bluetooth security have yet to be tested. However, the Bluetooth specification has a robust key management scheme built in, as well as upper layers of security. Bluetooth uses the national standard AES algorithm for encryption and the general consensus is that the options for Bluetooth security are strong and robust.

The Promise of Bluetooth – What it can do

The promise of Bluetooth is extremely ambitious. If Bluetooth lives up to its potential, it will revolutionize the way people interact with information technology. Originally conceived as a low-power short-range radio technology designed to replace cables for interconnecting devices such as printers, keyboards, and mice, its perceived potential has evolved into much more.

It has given rise to the concept of the Personal Area Network (PAN), a technology of convenience where everything within the Personal Operating Space (POS) of an individual that is related to communicating information (both voice and data) is automatically tied into a seamless peer-to-peer network that self-configures to make information easily accessible. Scenarios for its usage are many and diverse and are only limited by the imaginations of the companies that create the products.

Compared with wireless LANs

There is even talk of Bluetooth competing with WLANs, but Bluetooth products work over shorter distances and are designed to solve different problems. While the functionality of a WLAN device stands alone as a network component, the functionality of a Bluetooth component requires a host. The host can be any number of Bluetooth -enabled devices such as cell phones, headsets, keyboards, PDAs, vending machines, cameras, and bar code readers.

Usage model examples

Following are examples of some usage models for Bluetooth devices.

Wireless headset

The leading adoption of Bluetooth will initially be in the arena of mobile phones. Nearly every major mobile phone manufacturer has already released Bluetooth-enabled models of their popular phones. The driver for this adoption is the ability to use a wireless headset with the phone. The impact of mobile phone radiation on health has been under scrutiny for some time, especially since the phone is usually held near the head. The radio frequency energy emitted by a Bluetooth wireless headset is a fraction of that emitted by a mobile phone. Additionally, the convenience of being cordless means the phone can be used even if it is in a briefcase or the trunk.

Internet bridge

Bluetooth wireless technology can be used to allow a mobile phone or cordless modem to provide Dial-Up Networking (DUN) capabilities for a PC, allowing it to connect to the Internet without a physical phone line. This enables a laptop to automatically utilize the user’s nearby cell phone to dial and connect to a dial-up service. The user doesn’t need to touch the phone, which might be in a briefcase or coat pocket.

File exchange

The ability to perform peer-to-peer file exchange without the presence of a network infrastructure has many advantages. For example, a salesperson may choose to share the contents of an electronic slide presentation (as well as datasheets, business cards, and other electronic collateral) with the audience. Bluetooth enables the automatic detection of any Bluetooth devices in the room, enabling the transfer (with the receiver's permission) of all selected files. (This could also be done with a wireless LAN, but all parties involved would have to configure their clients to use compatible network settings. This is not required for Bluetooth.)

Synchronization

Bluetooth allows for data synchronization between devices. For example, a desktop computer that is Bluetooth enabled can wirelessly synchronize its contact list, task information, calendar, etc., to a user's phone, PDA, or notebook. Several Bluetooth-based synchronization models already exist for both Pocket PC and Palm-based PDAs.

Printing

HP is making printers and notebooks with embedded Bluetooth technology. Bluetooth-enabled devices can automatically detect Bluetooth-enabled printers in their area and wirelessly send documents to the printer without going through lengthy network and printing setup processes. Mobile users who frequently visit remote offices will find Bluetooth printing a significant improvement in convenience to their current experience.

An engineering challenge

The demands of creating Bluetooth-enabled products are very challenging. Consider the following:

- Bluetooth must have a very flexible application topology. For example, you might want your PDA to be able to communicate with any nearby printer, but do you want your cell phone to send its audio to any nearby hands-free headset?
- Bluetooth must be automatically configurable. If a Bluetooth product can't figure out whom it should and shouldn't talk to and how, the marketplace will consider it too complicated to use.
- Bluetooth must have quality of service (QoS) features to support voice.
- No one wants cell phones with shorter battery life, so the power required to support Bluetooth capability must be very low.
- No one wants PDAs that are larger, so adding Bluetooth capability to a device should not noticeably increase its size.
- In order to replace cables, Bluetooth cannot cost more than cables. This means that Bluetooth technology cannot add more than $5 to the cost of the host device.

The phrase “Wireless connections made easy,” which is printed on the cover page of the more than 1,500 pages of engineering specifications that define Bluetooth, means easy for the user, but hard for the engineers designing the products. For the reasons outlined above, Bluetooth presents some of the most demanding engineering challenges in the telecommunications arena, and products are only just now beginning to appear on the market.

Bluetooth™ Product Certification

The Bluetooth Special Interest Group[1] (SIG) is a group of companies that cooperate to define Bluetooth standards and qualify Bluetooth products. A product that has passed certain testing criteria can be stamped with the Bluetooth logo, assuring a certain level of interoperability.

Bluetooth Basics – How it works

Network Topology

Any Bluetooth device can be a *master* or a *slave*, depending on the application scenario. Bluetooth employs frequency hopping spread spectrum (FHSS) to communicate. 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* is formed by a master and up to seven active slaves. The slaves in a piconet only communicate with the master.

A *scatter net* can be formed by linking two or more piconets. When a device is present in more than one piconet, it must time-share and 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, as 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.

Service Discovery

The concept of *service discovery* is utilized to determine what kind of Bluetooth devices are present and what services they desire or offer. When a Bluetooth device requires a service, it begins a discovery process by sending out a query for other Bluetooth devices and the information needed to establish a connection with them. Once other Bluetooth devices are found and communication is established, the Service Discovery Protocol (SDP) is utilized to determine what services are supported and what kinds of connections should be made.

In order for the above to happen, devices willing to connect must be located. Some devices may be set up so that they are invisible. In this case, they can scan for other Bluetooth devices, but will not respond if they are likewise queried. Applications determine whether a device is connectable or discoverable, and thus applications determine the topologies of networks and their internal hierarchies.

ACL and SCO Links

Once a connection has been established between two devices an Asynchronous Connection-Less (ACL) link is formed between them. An ACL link provides packet-switched communication and is the most common link used to handle data traffic. A master has the option to change an ACL link to a Synchronous Connection Oriented (SCO) link. An SCO link provides a QoS feature by reserving time slots for transmission of time-critical information such as voice. A piconet can have up to three full-duplex voice links.

Standard profiles to enable usage models

The number and variety of different Bluetooth usage models mean that Bluetooth devices must call from a large collection of different protocols and functions to implement a specific usage model. In order to ensure that all usage models will work among devices from many different manufacturers, this collection of protocols and functions must be standardized.

Bluetooth profiles are standardized definitions of protocols and functions required for specific kinds of tasks. The current Bluetooth Standard 1.1 contains 13 profiles, with more being continually added. One or more of these profiles are utilized when implementing various usage models. Some profiles are dependent upon others. Some of the most basic are:

General Access Profile (GAP)

This profile is required by all usage models and defines how Bluetooth devices discover and connect to one another, as well as defines security protocols. All Bluetooth devices must conform to at least the GAP to ensure basic interoperability between devices.

Service Discovery Application Profile (SDAP)

The SDAP uses parts of the GAP to define the discovery of services for Bluetooth devices.

Serial Port Profile

This profile defines how to set up and connect virtual serial ports between two devices. This serial cable emulation can then be used for tasks such as data transfer and printing.

Generic Object Exchange Profile (GOEP)

GOEP is dependent on the Serial Port Profile and is used by applications to handle object exchanges. This capability is then used, in turn, by other profiles to perform such functions as Object Push, File Transfer, and Synchronization (see below).

Object Push

This profile is used for the exchange of small objects, such as electronic calling cards.

File Transfer

This profile is used to transfer files between two Bluetooth devices.

Synchronization

This profile is used to synchronize calendars and address information between devices.

New profiles not yet part of the standard include the following: a *Basic Printing Profile* to facilitate printing of text emails, short messages, and formatted documents; a *Hands Free Profile* to enable a mobile phone to be used with a hands-free device in a car; a *Basic Imaging Profile* enabling Bluetooth devices to negotiate the size and encoding of exchanged images; and a *Hardcopy Cable Replacement Profile*, used by devices such as laptops and desktop computers that utilize printer drivers.

Power Levels and Range

Most Bluetooth devices, dependent on batteries for power, are designated as class 3 devices and are designed to operate at a power level of 0 dBm (1 mW), which provides a range of up to 10 m. Class 2 devices can utilize as much as 4 dBm (2.5 mW) output power, and class 1 devices can utilize up to 20 dBm (100 mW) of output power. Class 1 devices can have a range up to 100 m.

Bluetooth class 2 and 3 devices can optionally implement adaptive power control. Required for class 1 devices, this mechanism allows a Bluetooth radio to reduce power to the minimum level required to maintain its link, thus saving power and reducing the potential for interfering with other nearby networks.

The Evolving Bluetooth™ Standard

The Bluetooth SIG

Since the original Bluetooth specification was published in 1999, more than 2000 additional companies have signed on as associate members, able to participate in development of future standards and extensions by contributing efforts to various working groups.

The Current Specification

The current specification, Ver. 1.1[2], defines a radio which operates in the unregulated Industrial, Scientific, and Medical (ISM) band as follows:

2.4 GHz, FHSS w/1600 hops/s over 79 channels: 1 Mbps

The fundamental elements of a Bluetooth product are defined in the two lowest protocol layers, the *radio layer* and the *baseband layer*. Included in these layers are hardware tasks such as frequency hopping control and clock synchronization, as well as packet assembly with associated FEC (Forward Error Correction) and ARQ (Automatic Repeat Request).

The *link manager layer* is responsible for searching for other Bluetooth devices, creating and tearing down piconets, as well as authentication and encryption.

Higher layer definitions include the Bluetooth profiles.

Enhancing the Specification

The Bluetooth SIG is currently working on a new specification, due for publication sometime in 2002. In the interest of maintaining backwards compatibility, most of this work is confined to describing new profiles.

> One of the most intriguing is a car profile that describes the use of personal devices like pagers, cell phones, and laptops in an automotive environment. Envisioned usages include the automatic adjustment of various settings in an automobile, such as seat and mirror positions and radio tuning, based on personal preferences stored in a Bluetooth device. Another profile would link a cell phone, car radio, and text-to-speech software on a laptop, to allow email to be spoken audibly over the car radio.
>
> In addition to developing new profiles, other working groups are developing extensions to enhance Bluetooth operations. The radio working group is developing optional extensions to the current Bluetooth standard that include higher data rates and handoff capability to support roaming, and the coexistence working group is collaborating with the IEEE 802.11 and 802.15 working groups to address interference concerns and ensure that Bluetooth can coexist in the same environment with WLANs.

The IEEE

The Bluetooth and PAN concept has now been embraced by the IEEE (which has trademarked WPAN™) in the work of the 802.15 group. However, the IEEE 802.15 group is confined to developing standards only for the lower two protocol layers of the OSI Reference Model[3].

Task Group 1 (802.15 task groups are differentiated by number) is working on the IEEE version of the Bluetooth standard, which will define Media Access Control (MAC) and Physical (PHY) layers for fixed, portable, and moving devices within or entering a POS (in this case 10 m) of a person who is either stationary or moving. The 802.15.1 standard is being developed to ensure coexistence with 802.11.

Task Group 2 is investigating and recommending practices to facilitate the coexistence of WPANs and WLANs. 802.15.2 is also addressing concerns of interference between Bluetooth and WLANs by developing a model to quantify their mutual interference.

Though strictly not operating modes defined by the current Bluetooth standard, other task groups are investigating high-rate and low-rate WPANs. Task Group 3 is defining a high-rate MAC and PHY that will allow data rates of at least 20 Mbps for multimedia applications. Task Group 4 is defining a low-rate (200 Kb/s and lower) MAC and PHY for devices such as toys, remote controls, smart tags, and badges.

Bluetooth and Windows XP

Microsoft® has announced support for Bluetooth in the next release of Windows® XP as follows:

> Microsoft is creating native support in the Microsoft® Windows® operating system for Bluetooth wireless technology. This support is entirely new and is not based on existing software from other companies. The specific delivery vehicles are to be determined.
>
> Microsoft supports the Bluetooth technology as a wireless bus, complementing USB and IEEE 1394. The goal for Microsoft software support is to Windows work with

> several types of devices that implement Bluetooth wireless technology, such as PC peripherals, PC companions, and devices bridged to network resources through a PC.
>
> Support for Bluetooth wireless technology is not in the first release of Windows XP, because there is not a sufficient array of production-quality devices that conform to the Bluetooth specification for Microsoft to test. However, Microsoft is actively developing support for Bluetooth technology and will ship this support in a future release. Quality, reliability and compatibility are principal ship goals for Windows XP, and Microsoft will not compromise on the customer experience.[4]

Bluetooth™ Security

Bluetooth security, when compared with WLAN security, is both more complex and simpler. It is more complex in the sense that there are many different options for security based on different application scenarios. It is simpler in the sense that, for the most part, they are transparent to the user.

With WLANs it is up to the network administrator to add security at higher levels. With Bluetooth, since the Bluetooth spec includes all levels, higher-level security features are already built into the devices when appropriate.

Bluetooth security includes both authentication and confidentiality, and is based around the SAFER+ encryption algorithm. SAFER+ is a block cipher, but in this application is implemented as a stream cipher. SAFER+ was thoroughly analyzed and tested during the NIST's search for a national encryption standard. Although some versions were found to have very minor weaknesses, the 128-bit version as used in Bluetooth is considered very strong.

Link layer security – keys and more keys

The Bluetooth Baseband (link layer) specification defines methods for both authentication and encryption that are subsequently utilized by higher layers.

These methods utilize a number of keys generated by a process that begins with three basic device entities: a public 48-bit device address, a random number generator, and a secret PIN which is either built into the unit by the manufacturer or programmed by the user. A typical PIN may consist of just four decimal digits. However, for applications requiring more security a PIN code up to 128-bits long can be entered.

The first of many keys is created the first time the Bluetooth device is installed on the host and is typically never changed. This is referred to as the *unit key*.

Authentication

When a Bluetooth *session* (defined as the time interval for which the device is part of a piconet) is initiated, a series of additional keys is generated. One of these keys, referred to as the *link key* or *authentication key,* is a one-time 128-bit secret key that is used only during that session. The process of authentication employs the encryption of a random number by each device to verify that each is sharing the same secret link key.

Encryption

If encryption is required by the application, an encryption key is further derived from the link key, a ciphering offset number, and a random number. While the authentication key is always 128-bits, the encryption key may be shorter to accommodate government restrictions on encryption, which vary from country to country. A new encryption key is generated each time the device enters encryption mode. The authentication key, however, is used during the entire session.

Application layer security

The Bluetooth General Access Profile defines three security modes:

Mode 1 is non-secure. Authentication is optional.

Mode 2 gives service-level enforced security. The service provided by the application decides whether or not authentication or encryption is required. The Bluetooth SIG has published the Bluetooth Security Architecture white paper[5] that defines a suitable architecture for implementing service-level enforced security on Bluetooth devices.

The white paper splits devices into different categories and trust levels, as well as suggesting three security levels for services. The utilization of a database is suggested for enabling the user to authorize devices to utilize only particular services. Because the implementation of security at this level does not affect interoperability, this white paper is advisory only, and is not part of the Bluetooth specification.

Mode 3 is link-level enforced security. Both devices must implement security procedures in order for a connection to be established.

In addition to the above modes, a device can be configured to not respond to paging, so that other devices cannot connect to it. Or it can be configured so that only devices that already know its address can connect to it.

Such numerous and complex levels of security are necessary to accommodate the large variety of different usage scenarios. It falls on the designers of Bluetooth products to ensure that the complexity of Bluetooth is hidden from the user, while still providing the user with necessary security options.

Appendix

Acronyms

ACL - Asynchronous Connection-Less
AES - Advanced Encryption Standard
ARQ – Automatic Repeat Request
FCC -Federal Communications Commission
FEC – Forward Error Correction
FHSS - Frequency Hopping Spread Spectrum
IEEE - Institute of Electrical & Electronic Engineers
ISM - Industrial, Scientific, Medical
LAN - Local Area Network
MAC - Media Access Control
Mbps - Megabits per second
NIST - National Institute of Standards and Technology
OSI - Open Systems Interconnection
PAN - Personal Area Network
PDA - Personal Digital Assistant
PHY - Physical (Layer)
PIN – Personal Identification Number
POS - Personal Operating Space
QoS - Quality of Service
SAFER – Secure And Fast Encryption Routine
SCO - Synchronous Connection Oriented
SDP - Service Discovery Protocol
SIG - Special Interest Group
USB – Universal Serial Bus
WLAN - Wireless LAN

References on the Web

[1] Bluetooth SIG, http://www.bluetooth.com
[2] Bluetooth specifications, http://www.bluetooth.com/developer/specification/specification.asp
[3] A good explanation of the seven-layer OSI Reference Model, http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/introint.htm#xtocid130454
[4] Bluetooth support in Windows XP, http://www.microsoft.com/hwdev/tech/network/bluetooth/
[5] Bluetooth Security Architecture white paper, http://www.bluetooth.com/developer/whitepaper/whitepaper.asp