Bluetooth* Architecture Overview

James Kardach Mobile Computing Group, Intel Corporation

Index words: Bluetooth, Piconet, IEEE, 802.15, PAN, Wireless, CMOS Radio, Data Access Points, Cable Replacement, WLAN, Global, Frequency Hopping, SIG

ABSTRACT

The Bluetooth* wireless technology was created to solve a simple problem: replace the cables used on mobile devices with radio frequency waves. The technology encompasses a simple low-cost, low-power, global radio system for integration into mobile devices. Such devices can form a quick ad-hoc secure "piconet" and communicate among the connected devices. This technology creates many useful mobile usage models because the connections can occur while mobile devices are being carried in pockets and briefcases (therefore, there are no line-of-sight restrictions). This paper provides a brief description of some of these usage models and explains how the Bluetooth architecture is optimized to enable them. But first, let us answer the question: why now?

Original Bluetooth market requirements dictated integration into small handheld devices (mobile phones and computers were key clients), low cost (long term cost of under $5 per connection point), high security, low power, and ubiquitous global use of the technology. There was no single cellular technology that could meet the global use requirement (there are five wireless phone technologies in the US alone). While WLANs had good ad-hoc networking capabilities, there was no clear market standard to pick (there are at least three varieties of IEEE 802.11 standards and a variety of other proprietary solutions in the market). Moreover, cost was too high for integration; there were no global standards, and integration into small handheld devices (like mobile phones) was a problem. As such it was decided to take a different approach: replace the cable from the "Network Adapter" (WLAN card or cellular phone) with a low-cost RF link that we now call Bluetooth.

Today the Bluetooth technology is the only specification targeted at this new market of cable replacement. Even the IEEE organization has recognized the need for wireless cable replacement technology and started the development of the 802.15 working group that focuses on this market (they call it Wireless Personal Area Networks). This specification is based on the Bluetooth technology!

INTRODUCTION

The Bluetooth technology was developed to provide a wireless interconnect between small mobile devices and their peripherals. Target markets were the mobile computer, the mobile phone, small personal digital assistants and peripherals. These markets were represented by the companies who created the technology: Intel, 3COM, Ericsson, IBM, Motorola, Nokia, and Toshiba, and were further supported by the 1,600 other early adopter companies.

The goals of the technology did not include developing another Wireless Local Area Network (WLAN) technology, for which there were already many in the market and many more being developed. Rather, whereas WLANs are designed to efficiently connect large groups of people over a common backbone, the Bluetooth technology was designed to connect mobile devices over a personal and private connection (in essence, to replace the cables carried by many mobile travelers).

The Bluetooth technology tries to emulate the cost, security, and capabilities of common cables carried by mobile travelers. The technology must be as secure as a cable (supports application/link-layer authorization, authentication, and encryption); must be manufactured for about the same cost as a cable (designed for eventual manufacture as a single-chip CMOS radio giving a long-term cost goal of $5 an end-point radio); must connect to a variety of devices available to the mobile user (seven simultaneous connections) and support data rates that are consistent with a mobile traveler's needs (1 Mega symbol per second data rates per piconet); must support many simultaneous and private connections (hundreds of private piconets within range of each other); must support the types of data used by mobile users (voice and data); and must be very low power and compact to support the small portable devices into which the technology will be integrated. Finally, the technology must be global as the mobile devices will travel and must work with devices found in other parts of the world.

USAGE MODEL

While the Bluetooth usage model is based on connecting devices together, it is focused on three broad categories: *voice/data access points, peripheral interconnects, and Personal Area Networking (PAN)*.

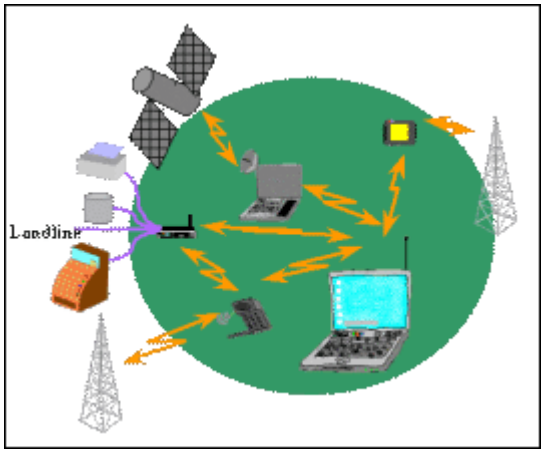

Figure 1: Voice/data access points

Voice/Data Access Points

Voice/data access points is one of the key initial usage models and involves connecting a computing device to a communicating device via a secure wireless link (see Figure 1). For example, a mobile computer equipped with Bluetooth technology could link to a mobile phone that uses Bluetooth technology to connect to the Internet to access e-mail. The mobile phone acts as a personal access point. Even more ideal, the notebook can connect to the Internet while the cell phone is being carried

in a briefcase or purse. The Bluetooth usage model also envisions public data access points in the future. Imagine the current data-equipped pay phones in airports being upgraded with Bluetooth modems. This would allow any mobile device equipped with Bluetooth technology to easily connect to the Internet while located within ten meters of that access point. These access points could, of course, support much higher data rates than today's modems, as public spaces could connect a variety of private Bluetooth access points via a LAN that is routed to the Internet over a DSL line, allowing each access point a private 1Mbps connection to the Internet.

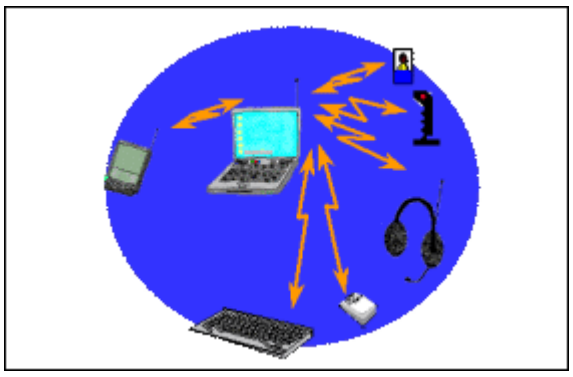

Figure 2: Peripheral interconnects

Peripheral Interconnects

The second category of uses, peripheral interconnects, involves connecting other devices together as shown in Figure 2. Imagine standard keyboards, mice, and joysticks that work over a wireless link. The Bluetooth link is built into the mobile computer; therefore, the cost of the peripheral device is less because an access point is not needed. Additionally, many of these devices can be used in multiple markets. For example, a Bluetooth headset used in the office could be connected to a Bluetooth access point that provides access to the office phone and multi-media functions of the mobile computer. When mobile, the same headset could be used to interface with the cellular phone (which can now remain in a briefcase or purse).

Another aspect of a short-range link like Bluetooth is in the area of proximity security devices. In this case, if one device is not within range of another device, the first device will go into a high-security mode.

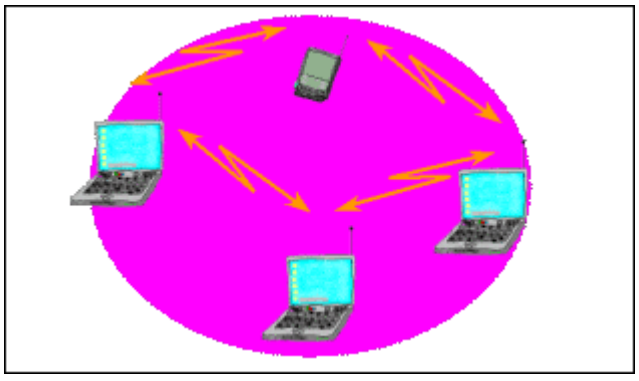

Figure 3: Personal Area Networking (PAN)

Personal Area Networking
The last usage model, Personal Area Networking (PAN), focuses on the ad-hoc formation and breakdown of personal networks (see Figure 3). Imagine meeting someone in an airport and quickly and securely exchanging documents by establishing a private piconet. In the future, Bluetooth kiosks could provide access to electronic media that could be quickly downloaded for later access on the mobile device.

THE DEVELOPMENT OF THE BLUETOOTH TECHNOLOGY

The Bluetooth technology was developed by members of a Special Interest Group (SIG). The participating companies agree not to charge royalties on any Intellectual Property (IP) necessary to implement the technology. The SIG started initially with the promoters, who were the primary developers of the technology, and then expanded to include early adopters and adoptees.

Environment
The Bluetooth technology was developed to be used within a unique global environment that would not only enable integration into the host devices but would also allow the mobile device to travel easily from one country to another. In addition, due to the personal/confidential data contained on the different types of client devices (e.g., the mobile computer), the link formed between these devices needed to be as secure as the cable it was replacing.

BLUETOOTH ARCHITECTURE

The Bluetooth technology is divided into two specifications: the core and the profile specifications. The core specification discusses how the technology works, while the profile specification focuses on how to build interoperating devices using the core technologies. This paper deals with the core technology, as illustrated in Figure 4, and focuses on the lower layers of the Bluetooth architecture (up to the link manager).

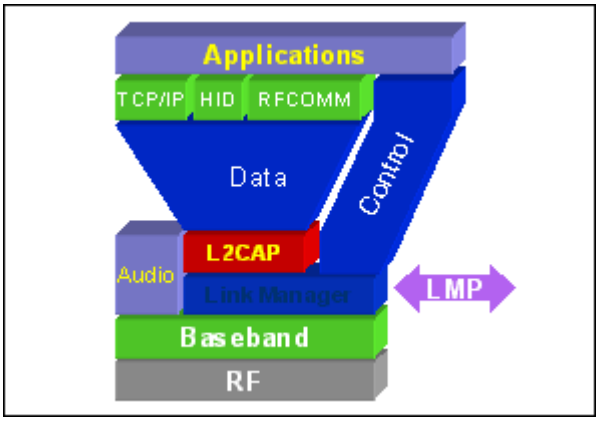

Figure 4: Bluetooth architecture

The Radio Frequency Layer

The Bluetooth air interface is based on a nominal antenna power of 0dBm (1mW) with extensions for operating at up to 20dBm (100mW) worldwide. The air interface complies with most countries' ISM band rules up to 20dBm (America, Europe, and Japan). The radio uses Frequency Hopping to spread the energy across the ISM spectrum in 79 hops displaced by 1MHz, starting at 2.402GHz and stopping at 2.480GHz. Currently, the SIG is working to harmonize this 79-channel radio to work globally and has instigated changes within Japan, Spain, and other countries.

The nominal link range is 10 centimeters to 10 meters, but can be extended to more than 100 meters by increasing the transmit power (using the 20dBm option).

The Bluetooth Baseband

As mentioned previously, the basic radio is a hybrid spread spectrum radio. Typically, the radio operates in a frequency-hopping manner in which the 2.4GHz ISM band is broken into 79 1MHz channels that the radio randomly hops through while transmitting and receiving data.

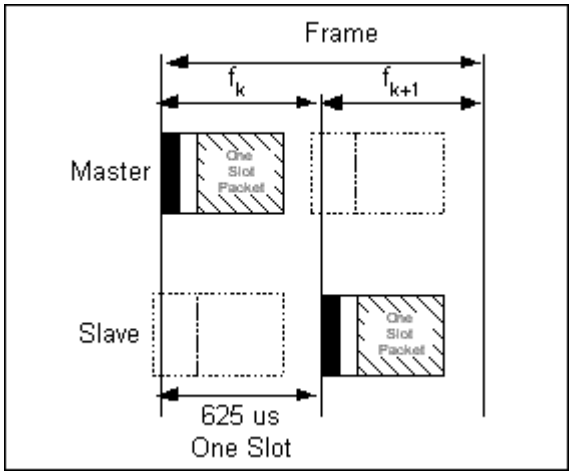

Figure 5: Single slot frame

A piconet is formed when one Bluetooth radio connects to another Bluetooth radio. Both radios then hop together through the 79 channels. The Bluetooth radio system supports a large number of piconets by providing each piconet with its own set of random hopping patterns. Occasionally, piconets will end up on the same channel. When this occurs, the radios will hop to a free channel and the data are retransmitted (if lost).

The Bluetooth frame consists of a transmit packet followed by a receive packet. Each packet can be composed of multiple slots (1, 3, or 5) of 625us. A typical single slot frame is illustrated in Figure 5, which typically hops at 1,600 hops/second.

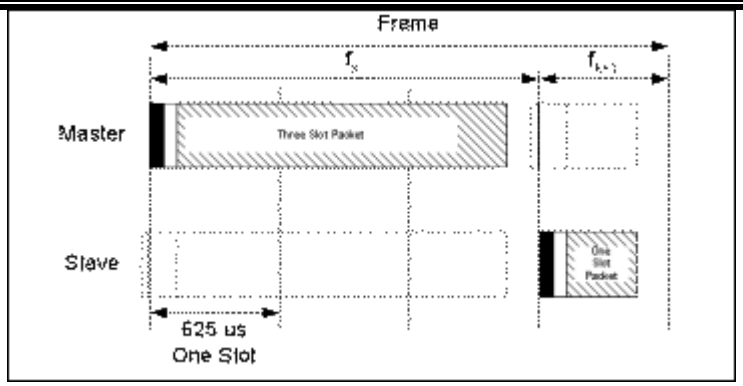

Figure 6: Multi-slot frame

Multi-slot frames allow higher data rates because of the elimination of the turn-around time between packets and the reduction in header overhead. For example, single-slot packets can achieve a maximum data rate of 172Kbps, while a 5 slot, 1 multi-slot frame will support a 721 Kbps rate (in the 5-slot direction) with a 57.6 Kbps rate back channel (in the 1-slot direction). A multi-slot frame is illustrated in Figure 6.

Network Topology

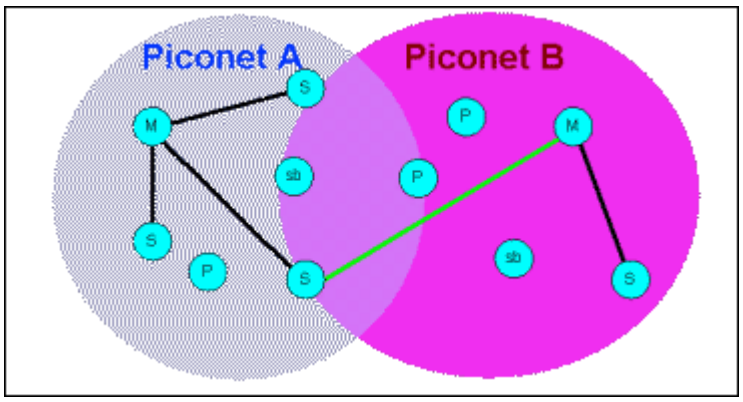

Figure 7: Network topology

Figure 7 illustrates a typical piconet with each small bubble (M, S, P, or Sb) representing a Bluetooth radio. Bluetooth radios connect to each other in piconets, which are formed by a master radio simultaneously connecting up to seven slave radios. The Bluetooth radios are symmetric in that any Bluetooth radio can become a master or slave radio, and the piconet configuration is determined at the time of formation. Typically, the connecting radio will become the master; however, a "master/slave swap" function allows the roles to be reversed. (A device can only be a master in one piconet though.)

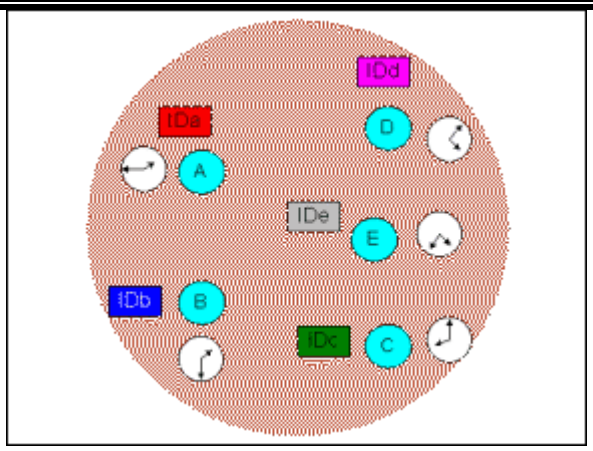

Figure 8: Bluetooth radios in the wild

To form a piconet, the Bluetooth radio needs to understand two parameters: the hopping pattern of the radio it wishes to connect to and the phase within that pattern. Bluetooth radios each have a unique "Global ID" that is used to create a hopping pattern. In forming a piconet, the master radio shares its Global ID with the other radios, which then become slaves and provide all the radios with the correct hopping pattern. The master also shares its clock offset (represented by the clock dial) with the slaves in the piconet, providing the offset into the hopping pattern. This information can easily be exchanged via the FHS packet.

Normally, radios not connected to the piconet exist in "Standby" mode. In this mode, the radios are listening for other radios to find them ("Inquire") and/or are listening for a request to form a piconet ("Page"). When a radio issues an Inquire command, listening radios will respond with their FHS packet (Global ID and clock offset), providing the inquiring radio with a list of Bluetooth radios in the area.

To form a piconet, a Bluetooth radio will page another radio with its Global ID (obtained by a previous inquiry). The paged radio will respond with its Global ID, and the master radio passes the paged radio an FHS packet. The paged radio then loads the paging radio's Global ID and clock offset, thus joining the master's piconet. Figure 9 illustrates Radio A becoming the master to Radios B and C.

Once a radio joins a piconet, it is assigned a 3-bit Active Member Address (AMA) allowing other radios on the piconet to address it. Once the piconet has eight radios active, the master must then take a radio and "park" it on the piconet. This radio stays coordinated with the piconet but releases its AMA for an 8-bit Passive Member Address (PMA). The freed AMA can now be assigned to another radio wishing to join the piconet. The combination of AMA and PMA allows over 256 radios to actively reside on a piconet, while only the eight radios with the AMAs can actively transfer data. This is also illustrated in Figure 9's Radio D, which has loaded the master's Global ID and clock offset and is parked on the piconet (prepared to join the piconet when data are ready to be transferred).

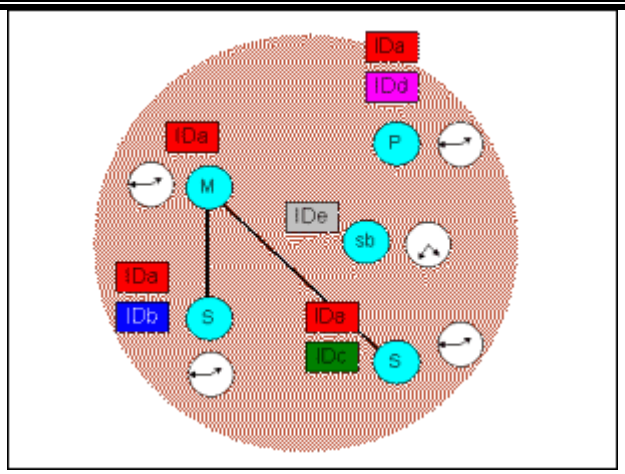

Figure 9: Bluetooth radios in a piconet

Parked radios listen at a beacon interval for information addressed to them. This allows a master to perform a broadcast to all slaves (parked and active).

Radios that are not actively connected to the piconet are in the standby state (e.g., Radio E in Figure 9). These radios listen for inquires or pages from other radios. Every 1.25 seconds they will perform a page scan and/or an inquiry scan to see if such a request is being made.

The inquiry process involves one radio executing a page function on the Inquiry ID (a special global address set aside for the inquire function), while other radios are performing an inquiry scan. This process is performed on a unique sequence of 32 channels. The radio doing an inquire scan will listen every 1.25 seconds on one of these 32 channels for 10 ms, then will repeat this scan on the next channel (within this 32-channel sequence). A radio with inquire scan enabled will continue this process until the inquire scan function is disabled. The inquiring radio will issue a number of pages on the Inquire channels (twice per single slot) and then listen at the corresponding response frequency (twice per slot) for 1.25 seconds for 16 of the 32 frequencies. The listening radio's correlator will fire if it is doing a Page Inquire on the same inquire channel as the inquiring radio and will respond with an FHS packet (containing its Global ID and clock offset). The sequence is then repeated for the second set of 16 frequencies after which the inquiring radio will have a list of FHS packets for all radios within range.

Paging follows a similar sequence. Each radio has a unique sequence of 32 paging frequencies and 32 response frequencies based on its Global ID. A radio in Standby mode doing a Page Scan will listen for a page of its Global ID on each of these paging frequencies for 10 ms, every 1.25 seconds going to the next paging frequency in the sequence. The paging radio will continuously page using the paged radios' Global ID on one of two sets of 16 frequencies within the paging radios' 32 paging frequencies. The paging radio makes an estimate (based on its last known clock offset) of where the paged radios should be listening and then creates an "A Train" of page frequencies around this estimated frequency. The paging radio will then continuously page across these 16 frequencies for 1.25 seconds. If the estimate was wrong (the paging radio received no response), the paging radio will next try the remaining 16 frequencies for the next 1.25 seconds. Radios that have little clock offset will be able to connect very quickly, while radios that have large clock offsets (meaning the

radios haven't connected recently) could take up to a maximum of 2.5 seconds to connect (a complete A/B Train search).

Once a radio has been found (via Inquiry) and then placed into a piconet (via Page), a piconet is formed and some useful work can now take place. Figure 10, entitled Functional Overview, depicts the different high-level states of a Bluetooth radio.

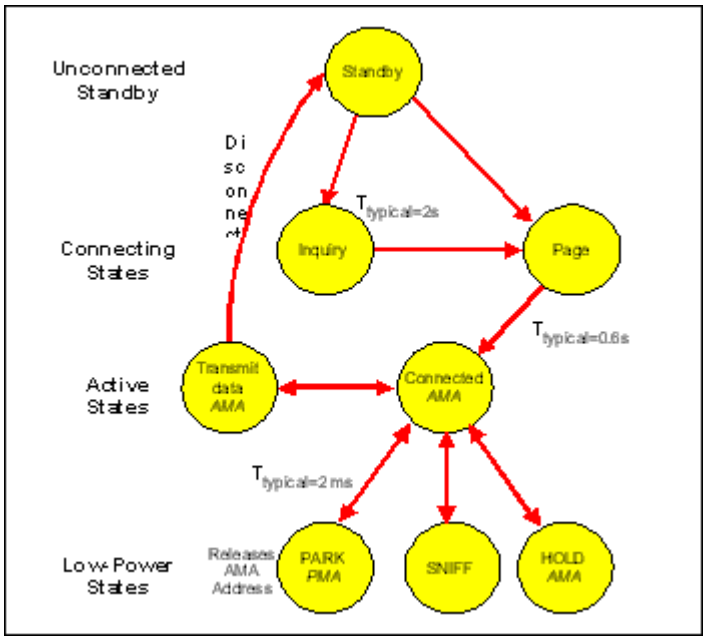

Figure 10: Functional overview

In the connected state, the Bluetooth radio is assigned a 3-bit Active Member Address (AMA) for which it can then direct data to different devices on the piconet (master is always referenced as address 0). Broadcasts to other radios on this piconet can be accomplished by the master sending a packet to address 0. To enable radios to maintain a connected state with the piconet (maintain the piconets hopping pattern and offset) while maintaining a very low-power state, radios can be placed in the Park, Hold, and SNIFF states. For the Hold and Sniff states, the radios are told to wake up at given intervals (go away for x slots); however, in the Sniff state the radio can transfer data on that interval (for example, a keyboard might be told to send/receive data every 20 slots), while in the Hold state no data are transferred. In the Park state, the radio is told to go away and is given the PMA address. A Parked radio will listen on a Beacon interval to see if the master has a) asked the parked device to become an active member, b) asked if any parked device wishes to become an active member, or c) sent any broadcast data.

When in the connected state, the Bluetooth radios can issue two types of packets: a Synchronous Connection Oriented (SCO) type or an Asynchronous Connectionless Type (ACL). The SCO type is associated with isochronous data, and, to date, this is voice. This is typically a symmetrical packet of 1, 2, or 3 slots, and the frames are reserved whether they are used or not within the piconet. In order to have an SCO connection, the radio must have already established an ACL connection. Once an SCO link has been added, a master or slave unit may send SCO packets without being polled.

Currently, the voice data links use a CVSD coding that provides very good noise immunity and a high-quality voice link. The CVSD coding enables damaged SCO packets to be thrown away (versus retransmitted) while maintaining a high-quality voice link. One baseband packet type allows both voice and data to be sent in the same packet (DV packet).

The ACL link is packet-oriented and supports both symmetric and asymmetric traffic. As mentioned previously, ACL packets are created with an odd number of slots such that the frame is always an even number of slots (1/1, 1/3, or 1/5, for example).

There are three error correction schemes used in the Bluetooth Baseband: 1/3 rate FEC, 2/3 rate FEC, and Automatic Repeat Request (ARQ). 1/3 FEC is always applied to the packet header information. To increase the data rate when the link gets noisy, the radio can start adding FEC to the channel: for SCO links, a 1/3 FEC is applied while for ACL links, a 2/3 FEC is applied. As mentioned previously, SCO packets are thrown away when damaged. However, for ACL packets, one packet is directly acknowledged by the recipient in the next packet.

SECURITY

The way that the Bluetooth radio system is used in mobile devices and the type of data carried on these devices (e.g., a corporate mobile computer) makes security an extremely important factor. While most wireless systems will claim that being a spread spectrum radio provides security, the volumes projected for Bluetooth radios eliminate this barrier. As such, link layer and application layer security are part of the basic Bluetooth radio requirements.

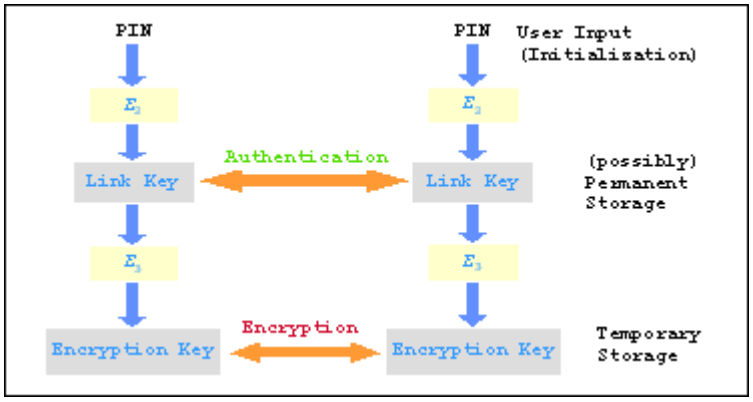

Figure 11: Link layer security architecture

At a link layer, the Bluetooth radio system provides Authentication, Encryption, and Key Management of the various keys involved. Authentication involves the user providing a Personal Identification Number (PIN) that is translated into a 128-bit link key that can be authenticated in a one- or two-way direction. Once the radios are authenticated, the link can be encrypted at various key lengths (up to 128-bits in 8-bit key increments). The link layer security architecture provides a number of authentication schemes and a flexible encryption scheme that allows radios to negotiate for key length. This is important, as radios from different countries will be talking to each other.

Security policies in these countries will dictate maximum encryption key lengths. Bluetooth radios will negotiate to the smallest common key length for the link (for example, if a USA radio is enabled for a 128-bit encryption key and a Spanish radio is enabled for only a 48-bit encryption key, the radios will negotiate a link with 48-bit encryption key). The Bluetooth architecture also supports authorization of different services to upper software stacks. For example, when two computers have created a Bluetooth link to exchange business cards, authorization must be created to extend these services (such that one computer could not examine other services on that computer unless enabled to do so).

The Bluetooth security architecture relies on PIN codes for establishing trusted relationships between devices. While not practical to go through all the combinations of uses of PIN codes, it should be noted that once a trusted pairing is established between devices, these codes can be stored within the device to allow more automatic/simple connections. The key to Bluetooth simplicity will be establishing the trusted relationship between commonly used devices. For random ad-hoc connections that require authenticated connections (such as ensuring you are connecting to who you think you are connecting to, something that is not always obvious with invisible radio waves), PINs would have to be exchanged (depending on how the devices are configured).

CONCLUSION

Bluetooth is a radio system designed for connecting a variety of mobile devices in a secure ad-hoc fashion. Much thought has gone into developing a radio system that provides interoperability between different device types while also meeting the requirements of mobile users. This paper covered a small aspect of the Bluetooth radio system, the lower layers of the Bluetooth radio stack.

ACKNOWLEDGMENTS

Thank you to the teams and companies that worked to develop this radio system in record time. These companies include, but are not limited to, Intel® Corporation, Ericsson, IBM, Motorola, Nokia, and Toshiba. Thanks to Laura Mariani for editing this article and Robert Hunter for reviewing it.

REFERENCES

[1] Bluetooth Specifications, Bluetooth SIG at http://www.bluetooth.com/.