OFFICE OF THE MANAGER
NATIONAL COMMUNICATIONS SYSTEM
TECHNICAL NOTES

Technology and Programs Division
Volume 7, Number 3
July 2000

Bluetooth Personal Area Network Technology

by Steve Karty

Introduction

The National Telecommunications Act opened new public access to the ultra high frequency (UHF) and very high frequency (VHF) bands. As a direct consequence, wireless local area networking is becoming the communications standard for small and mobile corporations. Hybrid networks composed of fixed and wireless assets appear to be the next step. An important aspect of these new wireless networks is the integration of household (and business office) appliances, laptop computers, and personal communications service (PCS) devices. The facile connectivity promised but unrealized by infrared (IR) technology may now be available via embedded omni-directional transceivers based on breakthrough radio technology chips. This technology, called Bluetooth, seamlessly connects each intelligent appliance in a household or an office in a piconet wireless network.

Bluetooth is an embedded, low-power, short-range, radio-frequency (RF) technology. Also, this mobile network technology is IR media-based with moderate bandwidth. It will

be a network-ready unit that meets the radio link, protocol, profile, and information requirements in the emerging standards.

Prospective Applications

Bluetooth will be most applicable for exchanging data between personal devices such as cell phones, radios, pagers, personal digital assistants, notebook computers, video and still cameras, audio players, and local area networks (LAN). The mechanism would support automatic synchronization of mobile devices when end users enter their offices. Figure 1 illustrates an example in which a camera transfers a photo object to a cell phone. Some writers also discuss the use of Bluetooth in household appliances, but the applications are unclear. Cell phone to cell phone relay is also considered practical (range permitting) as an alternative to the metered cell relay station.

Figure 1. Example Application, Cell Phone to Camera Data Exchange

Comparison of Technologies

With an operating range of 10 meters or less, Bluetooth's reach exceeds the current range of IR, but falls far short of other wireless networks. Implemented at 2.4 GHz in the Industrial, Scientific, and Medical (ISM) band, it has active and sleep mode power targets of 100 milliWatts and 100 microWatts, respectively. The Bluetooth developers are

attempting to keep the cost per unit at about $10 by using only a few, highly integrated chipsets that will make Bluetooth acceptable for small electronic devices.

The competition, IR, is represented by the Infrared Data Association (IrDA). With IR embedded in an estimated 100 million devices, it has become a de-facto standard. IR is presently a bi-directional data link, not a network, but efforts are under way to extend it to LAN and mobile implementations. The IrDA is also working on piconet protocols. A 100 Kbps link rate, usually split into smaller channels from 9.6 to 19.2 Kbps, will soon increase to 4 Mbps. The operating range is between 0.2 to 2 meters, depending on the power available. The limited distance and low power suggest that IR is most appropriate for small devices such as watches that would have a high production volume and thus a lower unit cost (approximately $5).

The 802.11 and 802.11b standards govern wireless networking as championed by the Wireless User Group. The range of wireless networking is typically 100 yards in open space, with a data rate of 3 Mbps and a frequency of 900 MHz, 2.4 GHz, or 5 GHz. Power requirements are on the order of 10 milliWatts, low enough for use in notebook computers. The current price of wireless network cards ranges in the hundreds of dollars. "Access point" devices cost about $1,500 each, however, amortization of the cost over seven or eight nodes makes them about $400 each. Table 1 summarizes this comparison information.

	IR	Bluetooth	Wireless
Range (meters)	1	10	100
Rate (Mbps)	1	1	3
Networked	No	Yes	Yes
Price/Node	$5	$10 Target	$400
Status	100 Million	Emerging	Here Now
Security	No	Level 2 Encryption	Level 2 Encryption
Standards	De-Facto	Specifications	Several

Table 1. Summary of Technology Comparison

With its projected performance and price parameters, Bluetooth fits nicely between IR and wireless technologies. Given that the American public wants its home appliances integrated, there is indeed a niche for Bluetooth.

Performance Design Goals

Meeting the very low power drain requirements with a 10-meter operating range, and implementing networking rather than just link communications, makes the design task more complex. However, engineering models of the radio and baseband unit have been successfully demonstrated, and only refinements remain to achieve the power level and range goals. Production engineering is expected to achieve the price goal.

The Bluetooth architecture integrates a combination of hardware and software into the networking device. The hardware is an embeddable module or a module residing on a card, which interfaces with the host device. It interfaces on one side with the host and on the other side with another Bluetooth device via its RF or IR transceiver. On the host side, there are four identified interfaces: the universal serial bus (USB), the PC card (or PCMCIA), and two serial interfaces, UART and RS232. All of these have established standards that define the physical and logical interaction. However, the higher level interaction between the Bluetooth device and the host is defined in unique Bluetooth protocols and packets.

The software includes salutation and security managers, a database, and the protocol stack. The transport technology is digital packet-oriented communications (rather than analog or streaming digital). Communication with the host includes hardware control and event monitor packet types. Asynchronous connection-oriented (ACO) and synchronous connection-oriented (SCO) packets are used for the link communication between devices, with SCO used primarily for real-time audio and video. Conventional packets, such as the Telephony Communications Service (TCS) and Internet Protocol (IP), are encapsulated in the Bluetooth SCO and ACO data packets, adding one more layer to the stack and therefore one more encapsulation with its overhead. Therefore, Bluetooth requires an additional protocol stack for a PC.

Figure 2 presents an example of the required additional protocol stack. The IrDa Object Exchange (OBEX) on the left side of the stack is required for IR interoperability. Next to it is a wireless network connection to a Bluetooth device that transfers data using a User Datagram Protocol (UDP) or Transmission Control Protocol (TCP). This figure shows how standard protocol encapsulation will occur.

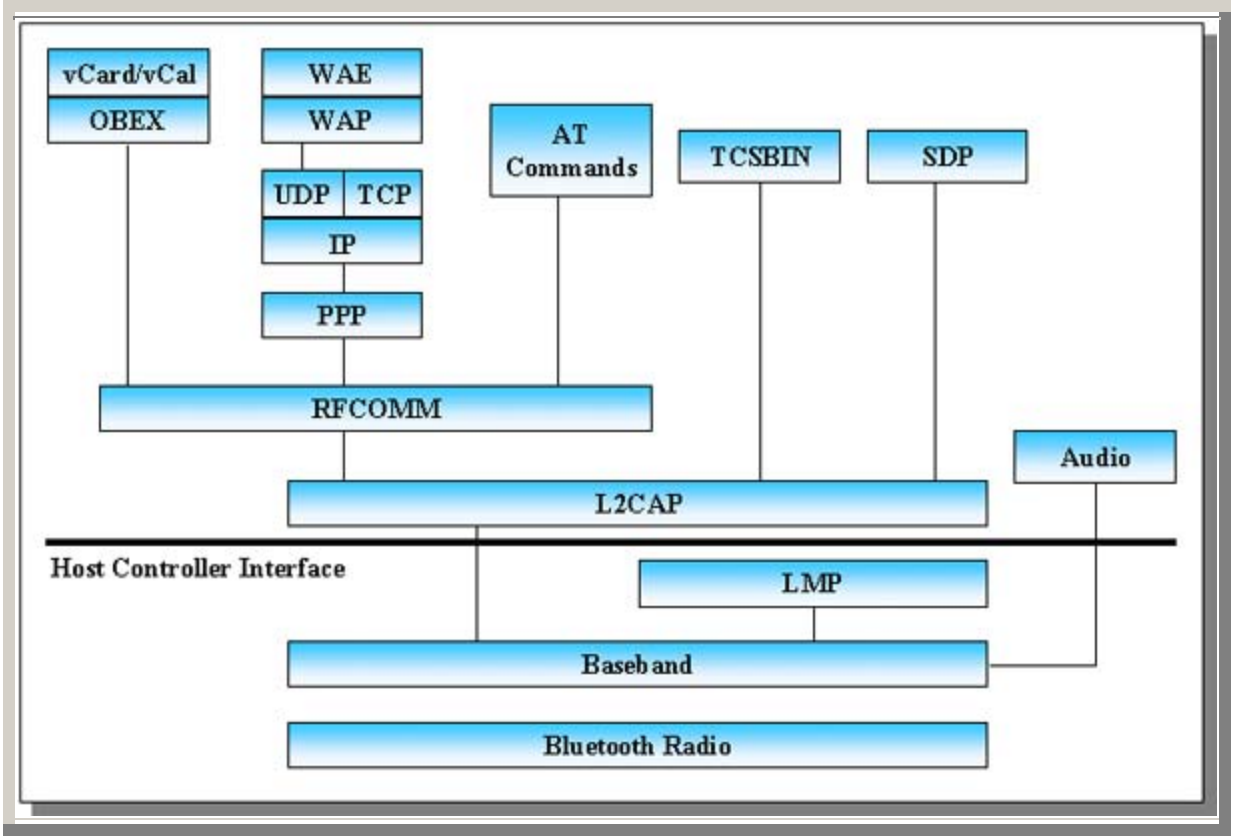

Figure 2. The Protocol Stack

Protocols, stacks, and a salutation manager provide Bluetooth "services." The salutation manager is like the old computer "monitor system," providing both server advertisement and client request capabilities, brokering the services, and establishing and then managing the follow-on communication session for the discovery function. The salutation manager is usually independent of the processor operating system and communication protocol. The actual data transfer is under host control via the protocol stack constructed for the data type.

The Bluetooth salutation manager has a subordinate security manager, which is invoked when discovery is initiated. The security manager holds service and device security databases. It consults these databases when a request comes in for services. It also submits identifying information when a request for services goes out to another Bluetooth device.

Security

One of Bluetooth's biggest selling points is its smart communications capabilities; devices automatically discover each other. The Service Discovery Protocol (SDP) is the means by which one Bluetooth device finds out about another. The device being discovered can be another Bluetooth product, a networked computer, or an Internet Web

site. Bluetooth devices are more compatible with the discovery function than other devices.

The discovery function is a source of security concern. Figure 3 depicts the database that holds the information and the security manager that makes the decisions regarding sharing that information during the discovery process.

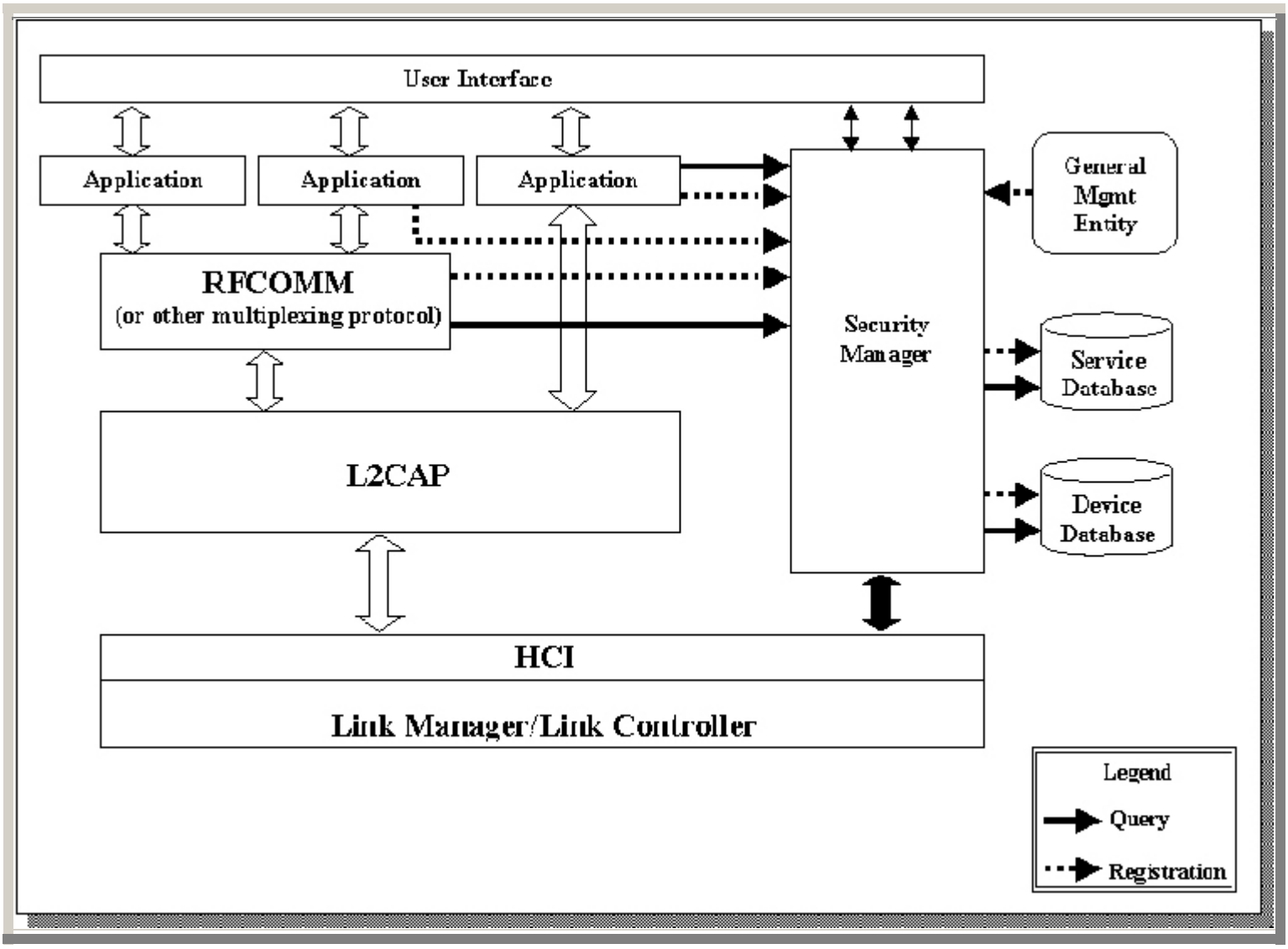

Figure 3. The Security Architecture

The process of service discovery occurs as follows. A client device either attempts to browse another device's server for information or it requests information about the server. It does this by providing a unique universal identification code. The queried device responds, depending on the security manager's decision, which is based on the device information in its database. If the device is a trusted unit according to the database, the requested information will be returned. How the database becomes populated with devices and trust information is beyond the scope of this paper. However,

human intervention and personal identification numbers are key to the development of trust and authentication information.

Further, security is only implemented at the logical link, which means it cannot address application-level security. Therefore, application-level communications security must be accomplished by the application itself. The device does not check every packet for security. Because the security manager develops trusted relationships, the device assumes a connection is secure and thereafter all communications are secure. Therefore, connectionless packets (e.g., UDP) are not security checked. Any security for a connectionless packet must be implemented at a level above (i.e., the application level) Bluetooth in the architecture.

Wireless networks also have security problems because of the degree of control at the physical level. However, assuming the physical layer can be penetrated without notice, wired and wireless networks have a lot in common. However, because wired networks have been around longer, managers have developed responses. Wired network security problems are addressed by a set of protocols and policies. Although some of the problems associated with the two kinds of are different, the managers of wireless networks can implement many of the protocols and policies formulated for the wired networks. Use of these protocols and policies could reduce wireless network security problems, including those of Bluetooth.

An Emerging De-Facto Standard

Bluetooth, now under development by a number of companies, is based on technology initially developed by Ericsson. As many as 1,400 organizations, industries, and companies worldwide now embrace the technology. Its sponsors include Intel, IBM, 3Com, Lucent, Microsoft, Motorola, Nokia, and Toshiba. Adoption by a preponderance of the industry would render Bluetooth a de-facto standard. However, it has not been adopted by any of the standards organizations (e.g., the Institute of Electrical and Electronics Engineers [IEEE], the Internet Engineering Task Force [IETF], and the International Telecommunications Union Telecommunication Standardization Sector [ITU-T]).

The IEEE 802.11 committee and Japan’s Nippon Telephone and Telegraph (NTT) are both investigating this technology for purposes of developing a standard. Some U.S. manufacturers are investigating their own implementations (e.g., GTE has "Body LAN"). Finally, the IrDA is proposing a new IR standard operating at 16 Mbps (dubbed VFIR for very fast IR).

When Will Bluetooth Appear?

Bringing the technology to market has been markedly slow since its announcement in May 1998 and projected debut a year later. In July 1999, the Chief Executive Officer (CEO) of 3Com announced that Bluetooth would be included in Palm Pilot VIII. Current

3Com documents do not address this subject. Ericsson, the initiator of the technology, was granted approval for a "module" in January 2000 and expects to receive approval from 15 other countries in March. More significantly, at demonstrations of partial Bluetooth technologies in December 1999, Extended Systems predicted it would be able to use its protocol stack technology this year. So far, there is no evidence that this prediction has come true.

Bluetooth technology fits nicely between the current IR and wireless networking, both in performance and cost. If the complete specification is implemented and if the price is comparable, Bluetooth could displace IR. Likewise, it might displace some of the shorter-range wireless networking. When or if this occurs, however, is a matter for the marketplace to sort out. Assuming Bluetooth comes to market, whether it becomes the dominant personal area network or just a niche product, is another question with a market-driven answer. Furthermore, the following security issues remain:

- The missing physical control of RF media
- The ad-hoc "discovery" capability of the technology
- Potential holes in the security manager if implemented
- Inability to secure third-tier situations even if a security manager is implemented.

A combination of security policies and network management security functions should reduce Bluetooth's inherent vulnerability to intrusion. However, development of those procedures and controls will take some time. Prudent management will initiate its own security precautions prior to the widespread adoption of piconet wireless technologies.

References

1. Telecommunications Act of 1996, § 207, Pub. L. No. 104-1-4, 110 Stat. 114, 1996.
2. Boyd-Merritt, Rick, "Blue Tooth group readies short-range RF LAN," *EE Times*, May 14, 1998.
3. Boyd-Merritt, Rick, "Short-range wireless camps seek common ground," *EE Times*, May 29, 1998.
4. Coates, James, "Pocket full of wireless miracles," *Chicago Tribune*, December 7, 1999.
5. Clarke, Peter, "Startup to add comm abilities to single-chip radios," *EE Times*, May 14, 1999.
6. Miller, Brent (IBM), "Mapping Salutation Architecture APIs to Bluetooth Service Discovery Layer Version 1.0," Doc. No. 1.C.118/1.0, White Paper, Bluetooth Special Interest Group, July 1, 1999.
7. Muller, Thomas (Nokia Mobile Phones), "Bluetooth Security Architecture Version 1.0," Doc. No. 1.C.116/1.0, White Paper, Bluetooth Special Interest Group, July 15, 1999.
8. Mettala, Riku (Nokia Mobile Phones), "Bluetooth Protocol Architecture Version 1.0," Doc. No. 1.C.120//1.0, White Paper, Bluetooth Special Interest Group, August 25, 1999.

9. Mettala, Riku, "Bluetooth PC Card Transport Layer Version 1.0," Doc. No. 1.C.123/1.0, White Paper, Bluetooth Special Interest Group, August 25, 1999.
10. Sonnerstam, Dan, et.al., "Specification of the Bluetooth System: Core," Volume 1, Doc. No. 1.C.47/1.0B, Bluetooth Special Interest Group, December 1, 1999.
11. Sonnerstam, Dan, et.al., "Specification of the Bluetooth System: Profiles," Volume 2, Doc. No. 1.C.47/1.0B, Bluetooth Special Interest Group, December 1, 1999.
12. "Infrared Data Association LAN Access Extensions for Link Management Protocol IrLAN," IrDA Web site [www.irda.org/standards/pubs/IrLAN.PDF].
13. "Infrared Data Association," IrDA Web site [www.irda.org].
14. "Technical Summary of IrDA DATA" and "IrDA CONTROL," IrDA Web site [www.irda.org/standards.asp].
15. "The Bluetooth Special Interest Group (SIG)," Bluetooth Web site [www.Bluetooth.com].

**Note: Graphics reproduced with permission from the Official Bluetooth Website [http://www.bluetooth.com/pressroom/photoarchive/photoarchive.asp]*.

For more information, please contact:

Steve Karty
National Communications System
Technology and Programs Division
701 South Court House Road
Arlington, VA 22204-2198
(703) 607-6188