EmbeddedSystems Conference San Francisco

An Introduction to Short-Range Wireless Data Communications
Thursday, April 24, 2003 – Class 325

Presented by:

Glade Diviney

Embedded R&D Manager, Extended Systems, Inc.

glade.diviney@extendedsystems.com

Abstract: A plethora of short-range wireless data communication solutions now vie for the attention of embedded designers. The current crop of contenders include IrDA, Bluetooth, 802.11b, and more newcomers than you can keep track of. These technologies cover a wide range of capabilities and constraints. Sometimes they compete and other times they complement. Who will win? Who will lose? Do there have to be winners and losers? This paper provides a survey of the broad range of short-range wireless data communication technologies currently available for embedded devices.

An Introduction to Short-Range Wireless Protocols

Ten years ago, the founders of the Infrared Data Association (IrDA) asked themselves a simple question: what's the best way to link two devices without a cable? This idea has now blossomed into several industries offering a bewildering assortment of products and protocols. In this introduction we'll explore the world of wireless communications mechanisms.

The three most popular standards for short-range wireless data communication are IrDA, Bluetooth, and Wi-Fi[1]. Each allows battery-powered devices to communicate without wires. Each is backed by an industry organization that manages a set of specifications and qualification programs. The similarities end there.

802.11 ("Wi-Fi")

The first IEEE 802.11 specification was introduced in 1997 with the primary goal of providing wireless LAN access. At first, component costs were expensive, interoperability was chancy, and security was a major concern. Together, these factors prevented widespread adoption. But, over time, component cost has dropped, many security concerns have been addressed, and new specification versions (such as 802.11b, 802.11a, and 802.11g)[2] have emerged that increase throughput. In 1999, the Wi-Fi Alliance was launched to certify implementations and alleviate consumers' interoperability concerns.

Because of the large physical range and "always-on" connection model, Wi-Fi technology consumes a lot of power, limiting its use in PDAs, phones, and other lightweight mobile devices.

Bluetooth

In 1994, Ericsson Mobile Communications began research on a radio module that could link mobile phones and accessories, especially headsets. Four years later, the Bluetooth SIG was launched by Ericsson, Nokia, IBM, Intel, and Toshiba, broadening the concept beyond mobile phones to include connections between PCs and other devices. Bluetooth-enabled wireless headsets started to emerge in 2000, but component cost, power usage, and even regulatory barriers prevented widespread adoption. Since then, cost and power usage have improved, making Bluetooth a valuable add-on feature for high-end PDAs and mobile phones.

---

1 Technically, these terms refer specifically to the organizations that manage the technical specifications. However, in practice, these terms are used interchangeably with the technology itself.
2 The Wi-Fi trademark refers to both 802.11a and 802.11b standards, however for convenience this paper focuses on the more widely deployed 802.11b standard.

IrDA

IrDA was launched in 1993 as a cable replacement technology using infrared light pulses. As the industry developed, IrDA realized that it was necessary to provide specifications that went beyond the basics of cable replacement. In early 1997, IrDA introduced the first version of the OBEX (OBject EXchange) protocol, allowing IrDA-enabled devices to wirelessly exchange business cards, calendar items, and other object types. A year later, 3COM's Palm III revolutionized the PDA world by allowing first-time users to easily swap applications and information. Today, nearly every PDA shipped supports IrDA, as do many mobile phones, laptops, printers, and other products.

Other Standards

Wi-Fi, Bluetooth, and IrDA implementations may be the most pervasive, but they aren't alone, especially in the Radio Frequency world.

HomeRF

HomeRF's target was home networking, providing file sharing, printing, internet access, gaming, and voice communications services between end user devices, with an emphasis on easy setup. Under constant pressure from the burgeoning 802.11 industry, the HomeRF working group was disbanded in January of 2003.

RFID

RFID is a wireless alternative to barcode scanners, allowing a component costing 25 cents or less to identify itself without a power source.

ZigBee

ZigBee, like Bluetooth, uses an unlicensed RF band for data communication, but targets applications that demand lower power, lower throughput, and greater physical range such as home automation, remote control, and device monitoring. Application-level specifications are still being produced and may be available mid-2003.

Ultra-Wideband (UWB)

Ultra-wideband uses a unique signalling mechanism that allows extremely high throughput (100 Mbps or more) using a simplified component design requiring very little power. Because UWB technology transmits over a wide swath of radio frequencies, it is unimpeded by the interference problems that obstruct traditional RF and infrared signals. UWB can also be used to pinpoint transponder location at a high resolution, and even "see" images through concrete walls.

So what's the catch? It transmits over many frequencies, including bands licensed only for military, aeronautic, and other restricted uses. UWB proponents argue that signals appear as background noise on any given frequency, but it may take years to achieve world-wide regulatory approval.

The relationship between UWB components and higher-layer protocols has not been fully resolved, although it is likely to be associated with the emerging IEEE 802.15.3 standard. The recently formed WiMedia Alliance shepherds the use of UWB in a communications environment.

Understanding the Differences

The three primary short-range wireless architectures, Wi-Fi, IrDA, and Bluetooth, have a great deal in common, but each has a unique set of strengths and weaknesses. In this section we will examine the major similarities and differences between them.

Speaking the Language (Protocol Architecture)

The venerable Open System Interconnection (OSI) Reference Model[3] describes the typical layers of any communications architecture. Short-range wireless architectures tend to be loosely modeled on the OSI "stack" of functionality as illustrated in the example below.

OSI Layer	Wi-Fi	IrDA	Bluetooth
7 – Application *(authentication, user services)*	File Transfer Protocol (FTP)	Point and Shoot Profile (PnS)	▪ File Transfer Profile (FTP) ▪ Generic Object Exchange Profile (GOEP)
6 – Presentation *(data format, encryption)*		Object Exchange Protocol (OBEX)	
5 – Session *(session management)*			
4 – Transport *(error recovery, flow control)*	Transmission Control Protocol (TCP)	▪ Tiny TP ▪ Information Access Service (IAS) ▪ Link Management Protocol (IrLMP) ▪ Link Access Protocol (IrLAP)	▪ RFCOMM ▪ Service Discovery Protocol (SDP) ▪ Logical Link Control and Adaptation Protocol (L2CAP)
3 – Network *(switching, routing, addressing)*	Internet Protocol (IP)		▪ Link Manager Protocol ▪ Baseband
2 – Data Link *(encoding/decoding, media access control)*	Ethernet (IEEE 802.11)		
1 – Physical *(signal)*		Infrared Controller, Transceiver	Radio Hardware

Figure 1. A comparison of wireless protocol architectures for file transfer applications.

The most important difference to note is the upper and lower bounds of each architecture. While protocol rules are always specified down to the physical layer, their upper bounds differ. A typical Wi-Fi architecture gives up control at the network layer to a standard TCP/IP protocol stack. Bluetooth and IrDA, on the other hand, each provide custom protocols that attempt to meet the unique needs of portable devices.

---

[3] See http://webopedia.internet.com/quick_ref/OSI_Layers.asp

Bluetooth and Wi-Fi differ wildly from the OSI model in one major respect. Because RF signals are easy to intercept, security procedures such as encryption are handled lower in the stack to enable lightweight applications. In both Bluetooth and Wi-Fi, security provisions have come under fire from users, who claim security features are too difficult to use, and security experts, who claim security features are too easy to circumvent. IrDA, perhaps wisely, stays removed from the security debate by claiming that infrared signals are much more difficult to intercept in the first place.

Bluetooth and IrDA share a significant difference from OSI and Wi-Fi in the concept of service discovery. To access an application service over Wi-Fi, a client typically sends a connection request to a specific TCP or UDP port. Bluetooth (via its Service Discovery Protocol) and IrDA (through its Information Access Service) both allow remote devices to query for available services instead of blindly guessing at them. In some cases, clients may also access additional information about a service, such as the availability of serial pin emulation when simulating a serial link, or the current load experienced by a network access point.

Making the Connection (Network Topology, Connectivity, and Range)

Topology begins with physical connectivity. In wired networks, connectivity can be taken for granted once the cables are plugged in, but in ad-hoc wireless networks, the question of "who can I talk to?" is non-trivial. In addition, "media access rules" must be defined to allow optimal use of half-duplex RF and infrared media.

IrDA Connectivity

IrDA physical connections are quite simple. Devices enter each other's 30 degree, 1 meter cone—in short, they are pointed at each other at relatively close range. One device (the *primary*) initiates a device discovery, and if a remote device (the *secondary*) is detected, it may initiate a connection. The two devices enjoy a simple, point-to-point connection at the fastest data rate supported by both devices. Generally, the connection is closed once the session is complete.
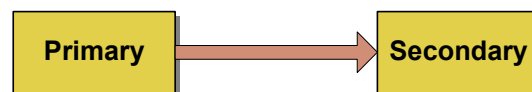

Figure 2. Typical IrDA Topology.

IrDA media access rules dictate that a device must wait for a 500 ms "media sense period" prior to assuming a primary role. This prevents devices from interrupting an existing connection. Once a connection is open, the primary sends data to the secondary, periodically offering the secondary a chance to transmit as well.

Wi-Fi Connectivity

Wi-Fi connectivity presents a star topology in which up to 32 clients all connect to the same network access point up to 100 meters away[4]. A portion of the 2.4 GHz RF band is utilized using a Direct Sequence Spread Spectrum (DSSS) scheme which handles interference by spreading data redundantely over a small range of frequencies. Connectivity is typically maintained until the device leaves range, is turned off, or (in the case of mobile devices) simply runs out of power.
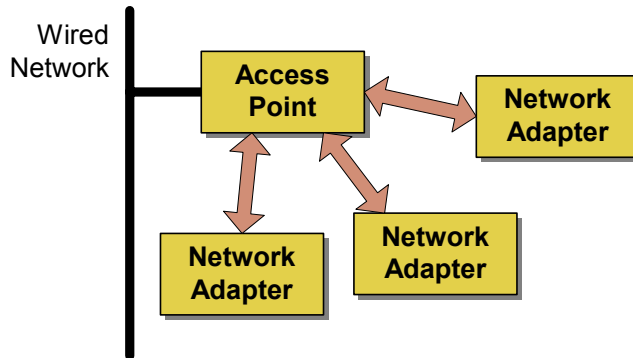

Figure 3. Typical Wi-Fi Topology.

Media access is generally unregulated; any device on the Wi-Fi network with data to transmit waits for a short period of silence (using a random back off timer to prevent collisions) and transmits. An acknowledgement packet (ACK) is sent to indicate that the data was received.

Bluetooth Connectivity

Bluetooth media access is based on a frequency-hopping scheme allowing many independent point-to-multipoint connections in the same physical space. Through separate *inquiry* and *paging* processes, a *master* device searches for and connects with a *slave* device in range, resulting in a *piconet*. To establish the connection, the slave must synchronize with the master's clock and pseudo-random hopping sequence before any data exchange can occur. This process can take up to 10 seconds but it can often be accomplished in less than 5.

---

[4] Wi-Fi devices may also offer an "ad-hoc" mode. However, the overwhelming majority of Wi-Fi use cases involve a mobile client connecting to a base station in infrastructure mode for network connectivity.

An interesting case arises when a master device must allow for new incoming connections. Such a device can advertise itself as a potential slave, and when a connection occurs, it may request a "master-slave switch," ensuring its role as master for all connections. The figure below illustrates the temporary *scatternet* that occurs in this case. The choice of master or slave roles is intentionally left unspecified by most profile specifications, with the intention that devices will create an appropriate piconet structure as the need arises.
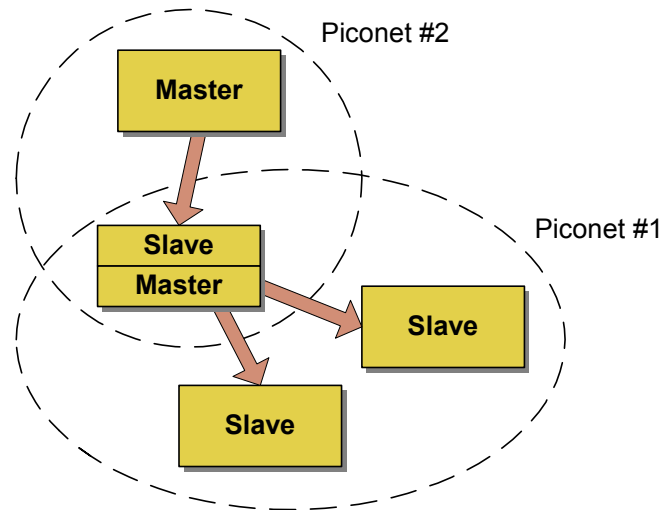

Figure 4. A Bluetooth Scatternet

Connections are either session-based (similar to IrDA) or maintained indefinitely (like Wi-Fi). Bluetooth allows additional connection states, known as *park*, *hold*, and *sniff*, which are used to minimize connection traffic, enter power-saving modes, or even to allow devices to temporarily participate in other piconets.

Media access is controlled entirely by the master, which periodically polls slaves for data.

The Need for Speed (Latency and Throughput)

We can separate aspects of wireless performance into several categories: *connection delay*, which is the time required to discover and establish connectivity; *communication latency*, which is the time taken to deliver the data through the network; and finally the *effective throughput*, which is the actual transfer speed (often much less than the native data rate allowed by the media). These performance characteristics are summarized in the table below.

	Wi-Fi	Bluetooth	IrDA
Connection Delay	2 seconds	Inquiry and paging take 2 to 10 seconds	Discovery and connection process takes 250 to 650 ms[5]
Communication Latency	< 10 ms	As good as 1.2 ms, worse if multiple connections or power saving modes are used	Typically < 20 ms, but may drop periodically to 500ms
Effective Throughput	Up to 4.5 Mbit/s (limited by interference, encryption)	400 Kbit/s, may be limited further by HCI and multiple connections	**115 Kbit/s links** (PDAs, mobile phones): throughput of 80 Kbit/s **4 Mbit/s links** (laptops, desktop IrDA adapters): throughput up to 3.5 Mbit/s

Figure 5. A comparison of wireless protocol architectures for file transfer applications.

It should be noted that Bluetooth system architecture often contains a bottleneck that limits effective throughput. Many Bluetooth implementations are separated into a *host controller* component (including the Link Manager, Baseband, and the radio hardware) and a *host* component (L2CAP, SDP, and other higher-layer protocols). This division allows Bluetooth host controller functionality to be embedded in firmware, while application-specific protocol layers execute within the device's CPU and operating system. The link between these two sides is known as the *Host Controller Interface* and is well-specified by Bluetooth. In many implementations, this interface is implemented as a serial link, limited to 115.2 Kbit/s and hence restricts effective throughput to a percentage of that speed.

Trading Latency for Throughput

Bluetooth chops its 1 Mbit/s data rate into tiny 625 microsecond slices. This hurts its effective throughput, but gives it two important advantages. First, it is resistant to interference at particular frequencies, since any given packet can be retransmitted quickly at a different frequency. Second, its low latency makes reliable, telephone-quality audio connections possible.

In IrDA, latency is variable, depending on how frequently the primary device polls the secondary. In many implementations, a period of polling with no data exchange causes the primary to back off its polling frequency to as long as 500 ms. This can sometimes cause a noticeable delay, but it also lowers power usage dramatically.

---

[5] Using IrDA's recently adopted Fast Connect mechanisms, connections can be established in as little as 100 ms.

Availability, Accessibility, and Interoperability

Metcalfe's law is often invoked to explain the success of the internet:

> *The power of the network increases exponentially by the number of computers connected to it. Therefore, every computer added to the network both uses it as a resource while adding resources in a spiral of increasing value and choice.*

With a few corollaries, we can apply this law to the value of short-range wireless technologies to their users.

Availability (Can you get one?)

First, for a connection medium to achieve exponential growth, it must be commonly available at reasonable prices. As an example, Wi-Fi networking equipment has existed for many years, it did not achieve widespread adoption until costs dropped to a point comparable to wired networks.

	Wi-Fi	Bluetooth	IrDA
Typical component cost	$20	$4	$2
Shipments (2002)	18 M[6]	48 M	118 M

Figure 6. The relationship between component cost and ubiquity.

Accessibility (Can you figure it out?)

Second, the technology must be relatively easy to set up and use. For example, 3COM's original Palm III leveraged IrDA's ease of use into a user-friendly operating environment. The result was a revolution in the PDA industry as first-time users were able to "beam" business cards and applications to each other.

IrDA protocols are the clear winner in the ease-of-use category. Connection parameters are negotiated at connect time with zero user configuration required. Bluetooth connections are slightly more complicated; first, device discovery is more complex because many Bluetooth devices may be in range. In addition, a one-time "pairing" process is often required, which may involve entering a PIN code on one or more devices. Wi-Fi is the most complex to set up, requiring configuration of SSID, WEP, Channel #, and other settings.

As a result, the most common users of these technologies tend to mirror their relative level of accessibility:

---

[6] In-Stat/MDR statistics

	Wi-Fi	Bluetooth	IrDA
Ease-of-use	Good	Better	Best
Typical use	Office user connects to corporate network with help desk support	Tech-savvy road warrior dials phone from PDA, transfers call to wireless headset	Grandma beams a recipe to mom

Figure 7. Ease of use and the typical consumer.

Interoperability (Does it work?)

Finally, we add the requirement for interoperability. Users expect devices of different types and from different manufacturers to be compatible with each other. Without interoperability, user's expectations drop and adoption rates are hindered. To prevent this outcome, all three wireless organizations have specific programs in place to achieve interoperability, with varying success.

These programs each include a mix of conformance testing, in which a device's behavior is analyzed by a protocol tester; and true interoperability testing, in which a device is tested against other real-world devices. The use of a logo or trademark is restricted to those who have successfully navigated a review process.

	Wi-Fi	Bluetooth	IrDA
Interoperability Program	Wi-Fi Certified	▪ Bluetooth Qualification ▪ UnPlugFests	IrReady
Typical Costs	$15k	▪ $5-10k for qualification ▪ $800 for UPF registration	<$5k
Number of Devices Listed	643	948	8
Number of Application Profiles Available	N/A	12+	4

Figure 8. Wireless interoperability programs (March 2003).

IrDA's relatively low listing number of listings (see the figure above) is attributable to the fact that the IrDA's qualification program ("IrReady") was made available only after many years of market adoption of IrDA standards. It has proven difficult for IrDA to replace the default "self-certification" process already in place with a new program of sufficient value to manufacturers.

Bluetooth and IrDA both offer "application profiles" which define the subsets of protocol functionality required to implement a particular user model. For example, IrDA offers the "Financial Messaging (IrFM) Point-and-Pay" profile, which explains how devices can exchange coupons, receipts, and of course credit card information. Bluetooth offers a host of audio, file-transfer, and telephony-related profiles.

Other Features

Keeping Your Data Safe (Security Features)

In short-range wireless, there are three primary aspects to security. *Authentication* allows a user to verify that the remote device is not being impersonated. *Encryption* encodes transmissions over the air to prevent eavesdropping, but not without a significant performance penalty. Each wireless architecture handles these issues in a unique way.

An IrDA user selects devices by physically aligning them. While this is sometimes inconvenient, it also provides a basic device selection and authentication mechanism. It would be very difficult to "spoof" an IrDA device since the malicious device would have to be in plain sight! Due to the close proximity of IrDA endpoints, encryption is rarely employed, since a device must be inside a 30 degree transmission cone to intercept the signal. One exception is considered in IrDA payment mechanisms, where many IrDA devices may be in a relatively small space. IrDA recommends that higher-layer encryption schemes be used to protect sensitive data (such as credit card numbers), but does not provide or recommend an encryption protocol.

Bluetooth provides both authentication and encryption algorithms at a very low layer (Baseband and Link Manager). Both schemes are based on link keys, which are derived from each device's unique Bluetooth device address, a user-determined PIN code, and a random value. To authenticate, devices simply demonstrate that they know one another's keys. Encryption is based on a linear feedback shift register (LFSR) scheme that can be fixed to any length between 8 and 128 bits to accommodate import/export regulations. To date, the Bluetooth encryption scheme has not been broken, but it is susceptible to poor PIN choice[7].

Wi-Fi relies on Wired Equivalent Privacy (WEP) for both authentication and encryption. However, a known flaw in WEP means that encryption can easily be cracked on busy networks. In fact, the official Wi-Fi Alliance web page on security[8] is mostly concerned with the additional technologies (such as VPN or 802.1X) that must be added to a Wi-Fi network to make it secure.

	Wi-Fi	**Bluetooth**	**IrDA**
Authentication	None	PIN key	Line-of-sight
Encryption	WEP (broken)	LFSR (not broken)	Limited range

Figure 9. Short-range wireless security mechanisms.

---

[7] When in doubt, try "1234"

[8] http://www.wi-fi.org/OpenSection/secure.asp

One other security feature of note is available within the OBEX protocol, which is maintained by IrDA and referenced by several Bluetooth profiles. OBEX provides an MD5-based user authentication mechanism, which is advised in cases where device authentication is insufficient. For example, a single device may have many users and offer different levels of access to different users, regardless of the device they use to connect.

Listening In (Audio Features)

Wireless audio services can roughly be divided into two broad categories: high-quality and low-latency. All three architectures provide sufficient bandwidth for high-quality audio to be exchanged. In fact, there are a variety of ways of streaming high-quality audio over any TCP/IP network, and the Bluetooth SIG is hard at work defining an "Advanced Audio Distribution Profile" allowing the same. IrDA has never made significant efforts in this direction, having been trumped by nonstandard and unsanctioned diffuse-infrared headset implementations.

The second category, low-latency, refers to the needs of a typical telephone conversation, in which wide frequency response is far less important than the immediacy of the audio. When audio signals in a telephone conversation take more than 100 ms on a round-trip, the delay becomes noticeable and the conversation becomes prone to accidental interruptions and awkward pauses. Wireless connections that add even a small amount of delay while processing and transmitting the audio signal may push the underlying phone connection into the latency danger zone.

Here, Bluetooth provides the most compelling solution. To be fair, IrDA proposed RTCON as part of its IrMC (Mobile Communications) protocol suite, and Voice over IP (VoIP) has been right around the corner for many years now. But adoption of these two technologies has been slow[9], while Bluetooth's low-latency SCO audio channels and power management features have made wireless phone headsets a viable consumer product category with more than a dozen entries on the market.

Making the Choice

With so many wireless technologies available, how can you decide on the right technology to use? To make the right choice, you must understand the benefits and limitations of each available technology and compare this to your application's needs. Below, we'll summarize some of the primary strengths and weaknesses of each wireless technology.

---

[9] http://www.itweek.co.uk/News/1138630

Wi-Fi

With its wide range and full leverage of the complete (if bulky) TCP/IP communications model, Wi-Fi is the obvious choice for office Wireless LAN connectivity. While you may be tempted to go beyond laptops and bring mobile devices such as PDA's into the Wi-Fi fold, power drain will likely thwart your plans. And if your data is even marginally sensitive, don't depend on Wi-Fi alone.

Bluetooth

Bluetooth trades away throughput and physical range for battery life and a low component cost. In the end it represents an ideal candidate for handling Personal Area Network (PAN) traffic, including local telephony, limited-range network connectivity, and other common uses.

IrDA

In cases where an ad-hoc, point-to-point data exchange is required, IrDA is the clear winner. IrDA is also capable of high throughput with low power usage and low component costs. Its relative ubiquity (IrDA is available in hundreds of millions of devices) may make it the right connectivity option when you need to interconnect with existing devices. Its line-of-sight model is suited to some applications (e.g., payment, simple object change) but not to others (e.g., networking, headset).

Glade Diviney is the R&D manager for the Universal Mobile Connectivity division of Extended Systems. His group develops portable, embedded source code kits for short range wireless protocols. Diviney served on Sun Microsystem's JSR-82 Expert Group that defined Java APIs for Bluetooth technology, and currently co-chairs the IrDA Test and Interop Committee. Glade holds a BS in Computer Science from Oregon State University.