Nearer My Peripherals To Thee

Short Range Wireless Comes of Age

By David Crowe

Short range wireless is a burgeoning field for research, standardization and real live products that extend wireless capabilities to applications within a few centimeters or meters of a person or a computer network in a home, office or factory.

Short range requirements make a good fit with unlicensed spectrum which is mostly in the bands above 1 GHz, especially the 2.4 GHz ISM (Industrial, Scientific and Medical) band. These higher frequencies provide shorter range, which is a problem for some applications, but a desirable feature for those that are naturally short range. Combined with low power, which is highly desirable for personal wireless devices, the risk of interference with wide area wireless devices is minimal. However, there is a risk that the proliferation of wireless protocols in the limited unlicensed spectrum will cause problems. There is special concern over the technology known as UWB (Ultra-wideband). Short range wireless devices will have to be designed to be relatively immune from other short range protocols as well as from emissions from higher power devices operating in or near the unlicensed spectrum ranges.

The history of short range wireless began in 1997 with the initial development of Bluetooth, although it was not until the turn of the century that Bluetooth really started to catch on. In fact, there were many naysayers in the late 1990s who thought that the protocol's promoters would eventually be crying the blues while spilling red ink. They were wrong, although the future of Bluetooth will not be without competing technologies hoping to encroach on its early market dominance. Judging by the number of different technical solutions that are available or planned, this is an area where one size does not fit all, at least not at present.

Bluetooth

Bluetooth was invented by the Swedish company Ericsson, and is named after Harald Bluetooth, a legendary Nordic king of the late 900s that all Swedes are taught about in grade school. There is no apparent connection between the king and the technology, except that the logo consists of the king's initials HB in Runic letters.

Bluetooth provides a "piconet" or PAN (Personal Area Network), connecting one master device with up to seven slave devices, commonly including mobile phones, keyboards, mice, wireless headsets and even personal ink jet printers. Some newer gaming systems include Bluetooth capabilities to connect game components together. Voice communication is supported, helped by the round-robin nature of scheduling to ensure that voice devices get adequate capacity even when other devices are transmitting large quantities of data. This is the most popular application for wireless phones, as it is usually Bluetooth that connects a wireless headset to a phone.

The first version of Bluetooth provided 1 Mbps of raw speed, which is certainly enough for some applications, although the 3 Mbps provided by the second version are beneficial when more devices are connected and when the data requirements are higher, such as when connecting a printer or cellular phone being used as a wide area network modem.

The future of Bluetooth is bright as it is now being built into many PCs, mobile phones and accessories. For consumers, Bluetooth makes a nice adjunct to their wireless environment. Many will be using Wi-Fi to connect their computer to their corporate LAN and the Internet, and, in turn, connecting using Bluetooth to connect it to all their peripheral devices.

Ultra-wideband (UWB)

Ultra-wideband is by far the most controversial technology for short range wireless systems because of its potential for interference. The Federal Communications Commission (FCC) in the US only approved the technology for use in 2002 after extensive consultation and after applying stringent rules in its first report and order (FCC 02-48). Industry

Canada kicked off discussions on the technology in February, 2005 with consultation paper SMSE-002-05. They have received considerable feedback on the issue but have not yet made a final ruling on how the technology can be used in this country.

Ultra-wideband uses short pulses of data transmitted over a wide frequency band, hence the fear of interference. The FCC does not classify a technology at UWB unless it uses at least 500 MHz of frequency, more than 10,000 times the bandwidth of an analog cellular channel (30 kHz). By spreading the signal over such a wide frequency band, UWB achieves very high data rates and extremely low power within the narrower bands used by other technologies. Although one device contributes only a tiny amount of noise to narrower bands, one interference fear is that large numbers of UWB devices could together significantly raise the noise floor for other radio systems.

UWB is oriented towards applications requiring higher bandwidth than Bluetooth, including large screens connected wirelessly to televisions, digital cameras and camcorders, and high speed data transfer between PCs and other devices. It also has applications that arise from its unique propagation characteristics that allow it to penetrate walls and even into the ground. This gives it benefits for data communications in some environments, but also means that the RF emissions are much less constrained than other short range wireless technologies whose transmissions are mostly line of sight and are easily stopped by walls.

UWB can be packaged in many different ways, so estimates of the performance when used as a data communications channel vary widely, but they are usually at least 100 Mbps and sometimes as high as 1 Gbps.

This high bandwidth has resulted in the adoption of the technology for Wireless USB, designed to provide a wireless link similar in capabilities to wired USB 2, but without the cables. UWB is also very popular in the arena of intelligent transportation systems (ITS) because of its radar capabilities, giving a vehicle awareness of its immediate surroundings even in bad weather.

The full potential of UWB will not be realized until all regulatory hurdles are overcome, which means that the major concerns over interference will need to be resolved. This will likely take several more years and even then configurations may be constrained to ensure that UWB is a good neighbour to other wireless protocols.

An attempt to standardize UWB in the IEEE, which has made a name for itself as a home for the standardization of unlicensed wireless data systems, failed due to an inability to resolve the differences between UWB and OFDM proponents. Consequently, IEEE Task Group 802.15.3a ceased operation. It is likely that standardization efforts will pick up again when the regulatory environment is clarified.

Zigbee

Zigbee is heading in the opposite direction from UWB, towards lower power (and bandwidth) than Bluetooth.

Unlike Bluetooth, which has one master device, Zigbee allows virtually any number of masters, although the majority of devices will act as slaves to reduce their complexity and power requirements. The technology is ideal for devices with a low duty cycle that transmit data only rarely, either when a special event happens (such as an alarm system or a pressure or temperature gauge with limit settings) or on a routine basis (such as a meter reader reporting hourly).

Zigbee devices should be able to operate from batteries for several years, unlike Bluetooth which is designed for devices that are frequently recharged. While Bluetooth devices will likely be providing capabilities to a central personal computer, Zigbee devices are more likely to be reporting via routers to a central server for automated monitoring of a house, office or factory.

This orientation to automation systems has made robustness in a high noise environment (such as a factory with high powered machines generating much EMF noise) an important factor in its design. Zigbee claims to be significantly more immune to noise than not only Bluetooth but also Wi-Fi.

Another focus has been to allow devices to quickly join and leave networks. Unlike Bluetooth, where a mouse may be connected to a computer for long periods of time, Zigbee devices are more likely to wake up, report and go back to sleep. Before they can report their information, however, they have to join the local network, something that Zigbee claims can be done in 30 msec. This speed is sometimes important for allowing events to be reported more promptly, but more importantly, for all devices, is that this limits the power consumption and extends battery life. A longer connection time would obviously require power consumption for a longer duration. Given that most Zigbee devices transmit short bursts of data relatively infrequently, a lengthy connection process would mean that more power would be consumed by the connection process than by actual data transmission.

Zigbee is designed to be so cheap that a bank of lights could include a device to communicate with a battery operated light switch, reducing wiring requirements in large buildings. It would also make it easier to control lighting centrally as all banks could be connected through the Zigbee network to a central control and monitoring system.

Wireless HD

Wireless HD is a technology backed by major Asian consumer electronics vendors for high speed communications between devices, including audio-visual home entertainment systems and PCs. Its proponents claim that it will be the high speed champion, with 2-5 Gbps transfer rates in the initial products and up to 20 Gbps in the future, which is more than even UWB can promise. By comparison, wired Internet access speeds in the era of modems were about one million times slower.

The technology will use the 60 GHz band. Due to significant line of sight

TECHNOLOGY COMPARISON

	Frequency	Data Rate	Peak Power	Range
Bluetooth	2.4 GHz	1-3 Mbps	1-100 mW	1-100 m
Zigbee	2.4 GHz 868/915 MHz	20-250 kbps	varies	5-500 m
ANT	2.4 GHz	< 1 Mbps	20-250 µWatts	< 30 m
Wibree	2.4 GHz	1 Mbps	n/a	10 m
UWB	3.1-10.6 GHz	100 Mbps - 1 Gbps	varies	10-20 m
Wireless HD	60 GHz	2-5 Gbps	n/a	10 m

constraints it will rely heavily on smart antenna technology. The initial concept (and at present it is just a concept) is that it will provide connectivity in one room, most likely to interconnect high-end home entertainment systems, connecting the high definition television and screen, cable interface, DVD player and game accessories together.

In this type of application, power requirements are not a big issue as most devices will still be wired into a power outlet even if they are not wired to each other. Raw speed, to provide high definition audio and visual, is the real aim.

At the time of writing, no specification was available from the initial partners, which include LG, Matsushita, NEC, Samsung, Sony, Toshiba and SiBEAM, however they were promising one by Spring 2007.

ANT – Nano Net Workouts

When the small Western Canadian company Dynastream (recently acquired by Garmin) developed a tiny device that could measure speed and distance in a running shoe a few years ago, they solved one problem, but created a bigger one – how to get this information to a device where the athlete could see it, perhaps in a watch around their wrist, or in a device pinned to a shirt or hanging round their neck.

Clearly the solution had to be wireless, but no protocols in existence at the time had the low power consumption and form factor that were needed. They developed the ANT wireless technology to solve this problem. Embedded in a shoe or watch and running off a coin-sized battery, the protocol can operate for several years in many applications. The design is optimized for low current when transmitting, the devices only transmit when necessary (one or a few times a second), and except for true ironmen (and women), the devices will only be in use for a small fraction of each day. Power consumption is measured in microwatts.

ANT has prospered in the market where enthusiastic athletes, amateur or professional, have become their own nano-network when working out with devices in their shoes, strapped to their chest, or all over their bicycle or exercise equipment.

ANT is still a proprietary protocol that is licensed to Dynastream customers, but there are rumors that it might eventually become a public standard (although standardization will not eliminate the need to pay license fees).

Wibree

Wibree is an attempt to broaden the reach of the Bluetooth technology to smaller power and form factor devices. By building on the Bluetooth RF interface, but adapting it to much lower power, the technology is extended to the point where it can be placed in devices like watches.

Wibree is a very young initiative, introduced by Nokia in October 2006. Although little information is currently available, it is clearly oriented at the same markets as ANT – sports and healthcare – but will also attempt to occupy a similar niche to Bluetooth in the home and office, providing lower cost devices with better battery life, although it is not clear it can quite achieve the extremely low power consumption of ANT.

A specification is promised in the second quarter of 2007.

Wi-Fi – 802.11

Wi-Fi does not really fit the classification of a short range wireless system, mainly because of its application as a general purpose Wireless LAN and because it usually relies on a base station (access point). However, Wi-Fi is important as the standard against which other unlicensed wireless protocols are measured. Since Wi-Fi can operate in a mode without an access point, if a job can be accomplished with Wi-Fi there would be no reason to design another protocol. Short range wireless systems have carved out niches beneath Wi-Fi, compensating for lower bandwidth with significantly lower power consumption and smaller form factors, and also above Wi-Fi, providing higher speeds for special applications. The IEEE 802.11 family is the king of the wireless LAN however, and it does not seem likely to be unseated from its position as the protocol best suited to the moderately fast interconnection of a large number of computers and shared devices, such as laser printers, internet routers and file servers.

RFID – Radio Frequency ID

RFID is also a form of short range wireless, but it is more oriented towards the identification of a nearby object (including animals and people). Though there is some overlap at the higher end of RFID devices, the technology generally assumes that an RFID tag will be brought within a few centimeters of a reader in order to scan its ID and possibly to obtain a small amount of additional information. By contrast, the general definition of short range wireless devices assumes that devices communicate from a static location or anywhere within a certain radius of other short range wireless devices and can communicate whenever the device decides that it needs to. Although RFID could be called "Ultra Short Range", it is really the nature of the application that is different. The extreme shortness of range is just a reflection of the need to bring an object near to a reader before communications can occur. RFID is most applicable when an object can easily be brought to a particular location to be scanned, such as an automated checkout counter at a supermarket, or a gate through which trucks enter and exit a port with tagged containers.

A Word on Security

Wireless systems almost always introduce the need for more security defenses than wired systems which often can rely on the physical protection of wiring. The importance of security varies with the application, and requirements are not always high.

Security breaches in personal area networks would allow information being transmitted wirelessly to be monitored, and could allow one device to be compromised and then used to worm into another. A wireless headset, if breached, could allow sensitive phone calls to be monitored, while systems that allow data connections could allow someone to break into a company intranet, for example. Intercepting wireless mouse communications, on the other hand, may be of very little value. Industrial systems are vulnerable to vandalism (e.g. shutting down a plant by interfering with its internal communications) or theft of proprietary information such as production information from meters. It is harder to think of attacks on home audio systems, although some people might not like their neighbours to know what kind of movies they watch.

One interesting security problem has emerged from England. It was found that thieves were monitoring for Bluetooth transmissions from vehicles before deciding whether it was worth breaking into them. For this type of attack, no ability to

crack communications is required – any transmissions in an unlicensed frequency band will tip off the crooks.

Some common sense is needed before deciding that short range wireless is just too dangerous to use. If someone is close enough to eavesdrop on your headset, they may well be able to hear the conversation. Talking loudly on a cellphone in a restaurant is a security breach that can only be resolved by the talker developing more concern for the importance of security (as well as more consideration for the majority of people who want to eat lunch and do not care about his company's sales figures for last month).

The most developed security systems are in Bluetooth and Wi-Fi unlicensed wireless systems. In both cases, their initial security systems were compromised. This caused standards groups to make significant improvements.

Security, while important, can come at a price in reduced usability. Make the pairing of two short range wireless devices too difficult, and they will be less desirable to consumers. However, when thoughtfully designed, it is possible to combine good security with good usability.

The Future

Looking into my crystal ball (an early example of a wireless communications device), I can confidently predict that the future of short range wireless will be filled with innovation and new protocols spiced with some failures. There is overlap in the low end, and some of the protocols that are currently good ideas may end up being abandoned. In fact, some already have. HomeRF, for example, was terminated in 2003 when it was squeezed by the widespread availability of IEEE 802.11b (Wi-Fi) on one side and Bluetooth on the other.

As short range wireless systems become more widely implemented, their limitations will become more apparent and then the protocols will have to evolve to survive, whether those new requirements are lower power consumption, greater range, less interference, higher bandwidth or smaller form factor. Protocols that cannot adapt will be replaced.

Short range wireless systems do not compete with public wireless systems – they complement them. Many cellular phones now support Bluetooth, for example, and in the future may also support other protocols to connect to accessories. These protocols may allow connection of a cellphone to a nearby computer, or for m-commerce applications using a cellphone to pay for a variety of products. The power of the protocols is enhanced when they work together. A possible example would be Bluetooth being used to communicate with a payment station, but the cellular portion of the phone may then be used to acquire a payment token from the cellular carrier to verify that payment has been accomplished, without having to supply any personal information such as credit card numbers. The payment station may use Zigbee to connect to the store's inventory system, and the product being sold may be a running shoe with ANT or Wibree, or perhaps a home entertainment system with Wireless HD.

Overall, the future of short range wireless in Canada and around the world is bright. We will be seeing many more products and systems based on this innovative group of technologies in the future. ■

David Crowe is a wireless standards, technology and numbering resource consultant based in Calgary. He can be reached at David.Crowe@cnp-wireless.com.