

Bluetooth Comes of Age  
James E. Bagley  
Code Corporation  
February 8, 2005

Many years ago, when the 802.11 standard was in formulation, a number of organizations were concerned that the requirements of WLAN protocols required too many handshakes for simple cable-replacement applications.

Indeed, preservation of a WLAN connection, and the control of roaming through a large facility, does require many transmissions that are not directly involved in data movement. Further, in an unplugged world, the movement of data from a non-intelligent peripheral such a headset or mouse precludes a complex protocol.

The Bluetooth Special Interest Group was formed to create a cordless transport method that would enable a wide variety of devices to enjoy the advantages of the low cost radios being developed for the 900 MHz - 2.4GHz ISM (industrial, Scientific and Medical) Band. The advantage (and disadvantage) of the ISM bands are that end users need not apply for a license from the airwave regulation authority (such as the FCC in the USA). This means that devices in the band must live with a variety of data and other noise in the band.

I remember the initial euphoria when industry leaders such as IBM, INTEL, and Motorola began placing Bluetooth devices on their product roadmaps. It was in 1997 that I first had an engineer promise me a cordless transmission method for our next generation of bar code readers that was "virtually free." Of course, "virtually" free is not free at all. The cost of a cable, although not insignificant, is still lower than everything else you need for cordless operation, such as batteries, chargers, and radios on each end. So the Bluetooth promise began to recede, and would not flourish until many other necessary technologies matured.

Take two-dimensional imagers, as an example. While this technology is taken for granted now, the power consumption of the first generation of these devices was such that a battery-powered version was impractical. The batteries needed to run the device were as big as the rest of the unit, and very heavy. Today we have low-power CMOS imagers and 400MHz processors that use a very small amount of energy. The latest generation cell-phone batteries have completed the price-performance side of the equation. So in 2002, when our newest generation of portable bar code readers was on the drawing board, the promise of Bluetooth again became an option.

We were still concerned about the wide availability of host-end radio support, but with the assurances of some WLAN veterans who had joined our engineering team, we took the leap. It was a worthwhile jump, although we found, when we landed on the other side of the proverbial technology chasm, that we needed to solve some basic problems that were not included in the licensed protocol stack. The most critical problem has to do with "applications level acknowledgement." The basic Bluetooth SPP (serial port profile) does not preclude packets getting lost in certain real world environments. We needed to add a layer of protocol at each end in order to assure our customers that bar code readings would not some how vanish into thin air without the user being made aware of the loss. We also found that getting input from a virtual serial port to an application was not a solved problem, either. So we wrapped both functions, along with some other product features, into a host-end software product, and also embedded the logic into a host-end hardware product that feeds Bluetooth data into a legacy PS/2 (keyboard) or RS-232 (Serial) port. Yes, the proverbial technology chasm was bridged, in our case, by revenue-producing optional products.

Bluetooth technology has become so ubiquitous that it is difficult, now, to find a notebook computer or PDA that *doesn't* have an embedded Bluetooth radio. However, there are still a number of issues, some real, some imagined, that give IT management pause in regards to widespread Bluetooth deployment.

### 1. Bluetooth will interfere with my WiFi system

As organizations have become reliant on 802.11 networks, the mere thought of introducing devices that chew up 2.4GHz bandwidth is a sacrilege. However, we have found that the devices coexist very well in such an environment, . Bluetooth 1.1 protocol has spread spectrum frequency hopping even without the latest and Bluetooth 1.2 protocol which provides for Adaptive Frequency Hopping. But with AFH (available on all of our products, even old ones with a firmware upgrade), the Bluetooth radios become even more WiFi friendly, by finding the WiFi traffic and avoiding it. They similarly avoid any other streaming source of noise, making the operation more robust.

Here is an excerpt from a recent article about AFH:

"By creating the Adaptive Frequency Hopping feature, the SIG has responded to industry requirements to better facilitate communication between various devices operating in the 2.4GHz ISM spectrum, thereby creating a more friendly environment where a wide variety of devices can coexist," said Microsoft's Wireless Architect Dr. Michael Foley.

Adaptive Frequency Hopping (AFH) was explicitly designed to reduce interference between wireless technologies sharing the 2.4 GHz unlicensed radio spectrum. Cordless telephones, microwave ovens and certain Wireless Local Area Networking (WLAN) technologies, including IEEE 802.11b and IEEE 802.11g, generally share the same wireless frequencies as Bluetooth wireless technology. AFH works within the spectrum to take advantage of the available frequencies without limiting the Bluetooth transmission to a set of frequencies occupied by other technologies. This 'adaptive hopping' allows for more efficient transmission within the spectrum, thereby providing the user with greater performance, even if using other technologies along with the Bluetooth wireless technology.

### 2. Bluetooth enables industrial espionage and is less secure than 802.11

Since my laptop can "see" other Bluetooth devices in the neighborhood, it is easy to eavesdrop on the transmissions. Wrong. When two devices get paired up and connected, the transmissions between them are automatically unavailable to other devices. See the attached white paper comparing security of 802.11 and Bluetooth.

### 3. Bluetooth is not a "standard"

While a defacto standard, it has not been incorporated under the IEEE 802 flagship; however, this is just a matter of time. As of now, with millions of Bluetooth connections in place, this communications protocol is only going to expand.

All one needs to do is use a search engine to find "Bluetooth" and you will see the widespread use of this technology. It is a critical, low-cost tool for automatic id users, and will continue to grow rapidly in the end user community.