Bluetooth® Wireless Technology:
Robust & Secure Connectivity for Cordless Scanning Applications

Executive Summary

- Bluetooth wireless technology is commonly being used around the world to replace other wireless networking infrastructures and wired interfaces in a variety of industry applications.

- Common misconceptions surrounding Bluetooth's security, interoperability with other wireless technologies and its overall robustness for communicating mission critical data has led some IT and Operations professionals to question its viability when compared to other wireless technologies such as WiFi.

- Now in its 4th generation and with an install base of over 500 million units, Bluetooth is a globally certified short-range communication technology that exhibits the security, data integrity and versatility to make it a safe and effective solution for communicating data wirelessly within the enterprise. Based on this, Bluetooth is confidently being selected around the globe for cordless scanning solutions.

Bluetooth In-Brief

Bluetooth wireless technology is a short-range communication technology intended to replace the cables connecting portable and/or fixed devices while maintaining high levels of security. The Bluetooth specification defines a uniform structure for a wide range of devices to connect and communicate with each other. The key features of Bluetooth technology are robustness, low power consumption, and low cost.

Bluetooth technology operates in the unlicensed industrial, scientific and medical (ISM) band at 2.4 GHz, using a spread spectrum, frequency hopping, full-duplex signal at a nominal rate of 1600 hops/sec. A benefit of utilizing the 2.4 GHz ISM band is its unlicensed availability in most countries.

The technology is now available in its fourth version of the specification and continues to develop, building on its inherent strengths — small-form factor radio, low power, low cost, built-in security, robustness, ease-of-use, and ad hoc networking abilities. *Bluetooth wireless technology is the leading short-range wireless technology on the market today shipping over five million units every week with an installed base of one billion units in 2006.*

Compatibility / Interoperability with Other Wireless Infrastructures

Bluetooth products can effectively co-exist with wireless local area networks (WLANs). This includes WiFi networks and the many other devices that operate in the Industrial, Scientific & Medical (ISM) band. Since 802.11 networks are widespread and based on the 2.4 GHz ISM band, these will be the networks where interoperability is most likely to be a concern.

Bluetooth and 802.11 do have the potential to affect one another as they both operate in the same frequency – however both systems

were designed to cope with this by detecting any errors in transmitted data and re-transmitting it. The integrity of the data is never compromised. Additionally, Bluetooth uses Adaptive Frequency Hopping (AFH) capability to help further avoid interference.

Bluetooth v1.2 technology's Adaptive Frequency Hopping (AFH) capability was designed to reduce interference between wireless technologies sharing the 2.4 GHz spectrum. AFH works within the spectrum to take advantage of the available frequency. This is done by detecting other devices in the spectrum and avoiding the frequencies they are using. This adaptive hopping allows for more efficient transmission within the spectrum, providing users with enhanced performance even if using other technologies along with Bluetooth. The signal hops among 79 frequencies at 1 MHz intervals, providing a high degree of interference immunity.

The placement of devices should also be carefully thought out. As the antennas for 802.11b and Bluetooth are placed closer to one another, the Bluetooth signal can be effectively "drowned." It is recommended that a minimum 3 foot (1 meter) separation between Bluetooth devices and 802.11 devices be maintained to prevent the drowning of a Bluetooth signal. Note that this does not apply when Bluetooth and 802.11 co-exist in a single hardware solution.

Situation Analysis: Compatibility with 802.11

The frequency hopping sequencing is different for Bluetooth versus 802.11, and this helps mitigate the impact of overlapping networks.

The Adaptive Frequency Hopping (AFH) component of Bluetooth v1.2 further enhances performance by mitigating collisions. AFH works by maintaining a status on each attempted transmission channel and records the failure of data being transmitted across those channels. When a channel is found to be losing data or there are collisions, the channel is marked and transmission is no longer attempted on that channel.However, in AFH mode, the device will keep a minimum of 20 channels open to transmission regardless of other activity in the ISM band.

Key Bluetooth Facts:

• Bluetooth wireless technology is geared towards voice and data applications

• Bluetooth wireless technology operates in the unlicensed 2.4 GHz spectrum – a standardized frequency band without any fees.

• Depending on the device class, Bluetooth wireless technology can operate over a range of distances:
>Class I: 330' (100m)
>Class II: 33' (10m)
>Class III: 3' (1m)

• Bluetooth technology is omni-directional and does not require line-of-sight positioning of connected devices

• The Bluetooth specification allows multiple modes of security

• Standardized Bluetooth profiles ensure interoperability between Bluetooth products

Physical Environment

There are several environmental factors that will impact the range of a Bluetooth device. A normal installation environment setting will result in typical Bluetooth expectations for range. Line of sight range can be greater, but the link becomes less reliable as a function of distance. However, as long as a link exists, the integrity of the data being transmitted will be maintained.

Placement of the Bluetooth host during installation of a cordless scanning solution does require forethought if maximum range is desired. Here are 2 examples of how base placement can affect linking:

If the Bluetooth host is placed in one location (Location A), and the scanner is placed at a 33 feet (10 meters) distance from that location (Location B) with a line of sight signal path, the scanner should be able to connect to the base regardless of scanner orientation. Much work has been done to attempt to optimize the omni-directionality of the scanner so that the scanner orientation will have minimal impact on network connectivity. (See Figure 1)

If there are impenetrable objects between the base (Location A) and the scanner (Location B), 2.4 GHz radio signals will bounce off of objects in a way that helps signal integrity. (See Figure 2)
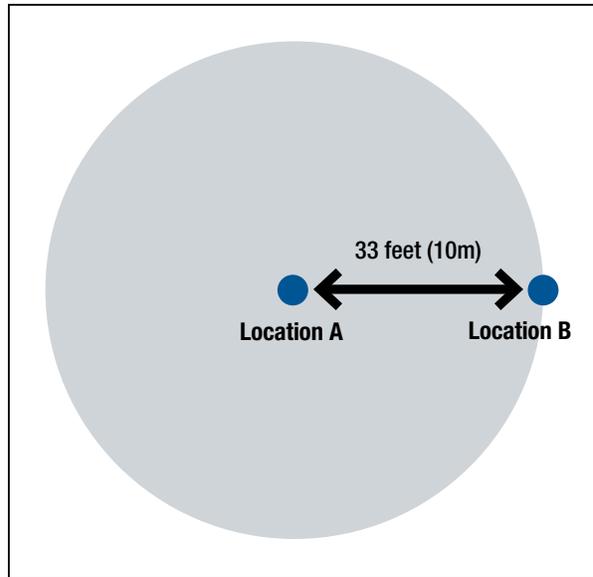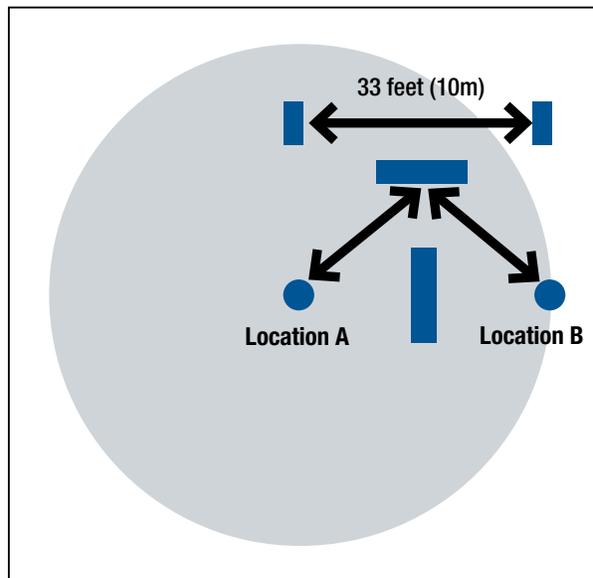

Figure 1

Figure 2

Security

Wireless standards the world over are evolving and have various formats for dealing with the security issues. Bluetooth wireless technology is no exception. Lately, confusion and misinformation surrounding security and Bluetooth wireless technology has increased. Current security issues typically involve mobile phones and cases where data has been compromised are the result of implementation issues on that platform.

Bluetooth technology has built-in security that includes 128bit encryption and PIN code authentication. When Bluetooth products identify themselves to a host, the host may require a PIN code the first time they connect. Should a PIN be required, they are always securely connected.

Product developers that use Bluetooth wireless technology in their products have several options for implementing security. There are three modes of security for Bluetooth access between two devices.

Security Mode 1: non-secure

Security Mode 2: service level enforced security

Security Mode 3: link level enforced security

It's important to note that the manufacturer of each product determines the security mode for their device. Therefore, manufacturers have the inherent ability to control how secure their Bluetooth device is.

Honeywell cordless scanning solutions are defaulted to Security Mode 3 - this means that the Bluetooth device is not "discoverable" to other devices. However, when the scanner is programmed to be discoverable, the host system may require a PIN to be entered before linking. This enables the highest level of security offered through the Bluetooth standard.

In Summary

Based on the global adoption of Bluetooth wireless technology across a wide range of applications, it's low-cost, low power consumption and built-in security features, Honeywell has standardized on this technology as the wireless platform for our cordless line of handheld imaging solutions. The security and robustness of data transmission offered by Bluetooth make it the right choice for customers who demand high-performance wireless data transmission within the enterprise.

For more information on Bluetooth wireless technology, visit www.bluetooth.com.

Honeywell