Wi-Fi… Why Now?
Exploring New Wireless Technologies for Industrial Applications

Patrick McCurdy
Product Marketing Manager
Phoenix Contact Inc.
pmccurdy@phoenixcon.com

Ira Sharp
Product Specialist
Phoenix Contact Inc.
isharp@phoenixcon.com
www.phoenixcon.com

KEYWORDS

Wi-Fi, Wireless Local Area Network, WLAN, Wireless Ethernet, Industrial Wireless, Industrial Ethernet, Wireless Security, Wireless Encryption, IEEE 802.11a/b/g, IEEE 802.11i

ABSTRACT

As Ethernet and Internet Protocol (IP) connectivity quickly become the "serial port" of the future it's clear that wireless technology trends will closely follow. Additionally, recently available spread spectrum technologies are enabling new applications that go beyond simple wire and conduit replacement to more data intensive and bandwidth demanding things such as video surveillance, in-plant VoIP, mobile computing, and active RFID asset tracking to name a few.

This paper will focus on the industrial use of public standard IEEE 802.11 technology while providing a broad comparison of different spread spectrum wireless technologies currently deployed in industrial automation applications. Sometimes called Wi-Fi, WLAN, and Wireless Ethernet, devices based on IEEE 802.11 standards are now part of the IT mainstream with many office and even home installations existing today. Advances in enhanced security features, data transmission reliability and environmental packaging have just recently made, what some thought of as a strictly commercial solution, appropriate for demanding industrial applications. Further more, higher powered industrial solutions and new antenna technology mean high data rates at impressive distances can now be achieved. Several application examples will be shared.

Presented at ISA Expo 2006; http://www.isa.org

Perhaps the biggest concern of industrial automation users regarding public standard technology such as IEEE 802.11 is if security of their network and automation system will be somehow compromised. Considerable attention will be spent on discussing solutions to these security concerns.

Introduction

As Ethernet and Internet Protocol (IP) connectivity quickly become the "serial port" of the future its clear that wireless technology trends will closely follow thereby providing ever greater network and data access. Wireless Ethernet capabilities via technology based on public standard IEEE 802.11 has gained mass commercial success. A quick look at available wireless networks from your laptop in virtually any public place or even your residential neighborhood is sure to find few. However, because a technology is approaching critical mass in the commercial world is it ready for use in industrial applications? While this question has been asked and answered regarding wired Ethernet (yes) it still remains a viable question regarding wireless applications. In addition to providing a broad comparison of different spread spectrum wireless technologies currently deployed in industrial automation applications, this paper will explore the industrial use of public standard IEEE 802.11 technology. Some basics of IEEE 802.11 protocol and application will be reviewed including a detailed discussion of security concerns and solutions. Finally several successful industrial applications of IEEE 802.11 technology will be discussed.

Spread Spectrum Technology

Wireless is a shared medium; therefore different techniques must be employed to assure that multiple signals can coexist in the same frequency range. The allocation of frequency for different uses is typically the role of government agencies. In the United States this agency is the Federal Communication Commission (FCC). Typically government agencies set aside some spectrum for public use. This public use must be shared by different users and applications; therefore for unlicensed applications there is typically a limit set for the power that can be transmitted and additionally some type of spectrum spreading technique is necessary. The allocation of frequencies requires sharing of frequencies when at all possible.

The requirement for spread spectrum in unlicensed applications is a good thing in terms of robustness and reliability for industrial applications. Spreading the communication over a wider frequency range means that the signal transmission is less effected by EMI or RFI emitted from industrial equipment, from licensed users, or from unlicensed radios. Three spreading or modulation techniques commonly used in spread spectrum radios will be discussed next. These include; Frequency Hopping Spread Spectrum (FHSS), Direct Sequence Spread Spectrum (DSSS), and Orthogonal Frequency Division Multiplexing (OFDM).

FHSS radios take a piece of information that needs to be transmitted and divides it up into small packets. The packets are then transmitted across the band by selecting pseudo-random frequencies within the band. The bit of information is transmitted at one frequency and done so with a lot of power, giving it the ability to overcome many sources of noise that may arise. Packets are transmitted

as signals on different frequencies and upon receipt the signals are checked for errors. Interference is effectively addressed by the complex transmission of data packets. Although interfering signals can knock a packet out of a FHSS signal's hop pattern, the rest of the updates generally reach the receiver, no matter how powerful the interference. Therefore it's often said that FHSS technology "tolerates" interference. In addition, transmitting small targets that constantly and randomly jump frequencies makes it almost impossible for someone to tap into the signal. The robustness of the data transmission makes technology based on FHSS very attractive for the high EMI / RFI world of industrial applications.

DSSS radios continuously spread data across a wide portion of the frequency band and rely on processing to address interference. The information is again divided into individual packets but now grouped together with a bit sequence which is called the chipping code. This effectively takes the packets of information and divides them up into several segments, essentially making one piece of information become several pieces of information. These pieces of information are then transmitted at the same time across a series of frequencies called a channel. This is done because the series of information can be transmitted at a much lower power then the FHSS technique. With DSSS multiple packets of information are transmitted at the same time therefore faster transmission speeds are possible. If one or more bits are damaged due to interference during transmission, the data will be restored; however, this will likely decrease the transmission speed or overall performance. Providing limited protection against interference, DSSS radios can lose data if excessive noise or other equipment on the same bandwidth interferes with the signal. DSSS moves many bits per second and is typically used for IEEE 802.11b high-speed radio applications.

Lastly OFDM is done by once again dividing information into packets. Next, those packets are again broken up into smaller packets and transmitted across a series of frequencies similar to DSSS but now in smaller chunks. These smaller chunks of data are transmitted simultaneously allowing for much greater speeds then that of FHSS or DSSS. See Figure 1 for a comparison of FHSS, DSSS, and OFDM modulation techniques.

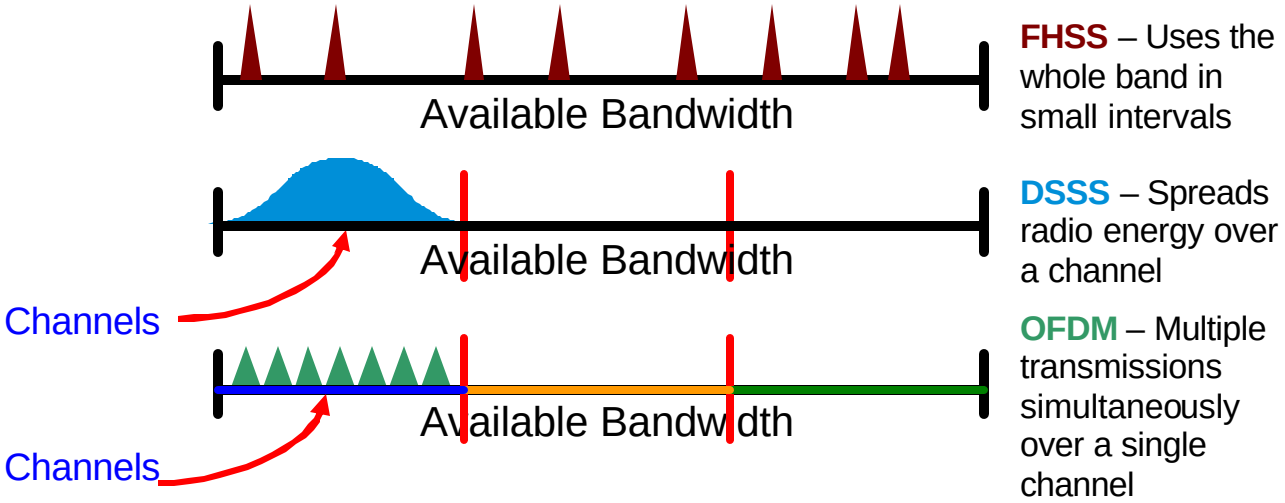


Figure #1 – Comparison of Modulation Techniques

ISM Frequency Bands

In the United States there are 3 frequency bands that are set aside for public use without a FCC license. These are the so called ISM (Industrial, Scientific, and Medical) bands: 902MHz – 928MHz, 2.4GHz – 2.4835GHz, and 5.15GHz – 5.850GHz. It's important to note that the 2.4Ghz band is generally accepted globally as an unlicensed band with limited transmit power. This power limitation typically equates to 100mW on IEEE 802.11 products. However, in the U.S. the power allowed is greater which generally means in unlicensed applications output power ratings up to 1Watt are allowed. Industrial IEEE 802.11 solutions are available in the U.S. with higher power rating then the universally accepted 100mW. In general all three bands have their place in industrial applications each has its potential strengths and weaknesses as reviewed in Figure 2. .

Frequency Band	Advantages	Disadvantages	Comments
900MHz (902 - 928 MHz)	* More robust, less 900MHz Interference sources * Lower attenuation, travels further through obstacles.	* Low bandwidth prevents larger data transfer means slower speed.	* Not available internationally.
2.4GHz (2.4 - 2.4835 GHz)	* Higher bandwidth allows large data transfer and faster speed.	* Attenuates quickly preventing propagation through obstacles. * Large amount of 2.4GHz traffic.	* Accepted globally meaning typically lower component costs due to economies of scale.
5.8GHz (5.15 – 5.25 GHz) (5.25 – 5.35 GHz) (5.725 – 5.850 GHz)	* Highest bandwidth allowing large data transfer and fast speed. * Least congested unlicensed RF band	* Attenuates very quickly meaning low propagation through obstacles and requiring special low loss cable and high gain antennas.	* Not available internationally. * Good alternative to 2.4GHz when high 2.4GHz traffic causes interference.

Figure #2 – Comparison of ISM Frequency Bands

Public vs Proprietary Wireless Technologies

Interoperability and Wireless Standards are two connected subjects that are often discussed when speaking about Industrial Wireless applications. Interoperability refers to the ability of different devices to communicate and understand the same "language" between each other even when these devices are from different manufacturers. Industry recognized standards facilitate interoperability among different manufacturer's equipment. Proprietary technology refers to one particular

manufacturer's modulation algorithms, interface, and over the air techniques. Therefore, typically one particular manufacturer's proprietary technology equipment will only work with other equipment they manufacture. This creates a formidable security barrier as only "insiders" have access to the particular technology; however, interoperability does not exist. An example of a proprietary wireless technology is the Phoenix Contact's Omnex Trusted Wireless technology used in Wireless I/O and Serial Data products. Public standards are agreed upon by a governing body that exists to create or certify a specification to guarantee interoperability between manufacturer's devices. Public standards mean that the radio "language" is known and therefore interoperability should be guaranteed. Since the communication parameters are public information, issues related to security are of a major concern. Therefore, encryption and authentication are the only form of security mechanism for public standard technology. Examples of public standard wireless technology include Bluetooth and IEEE 802.11a/b/g.

IEEE 802.11

IEEE 802.11a/b/g actually describes three variants of the wireless Ethernet standard currently implemented in commercial and increasingly industrial applications. These three variants are based around the same physical layer of the OSI model and in part define what band the wireless network will use along with the modulation technique. Additional jargon used to describe devices based on IEEE 802.11 standards include "Wi-Fi", "W-LAN", and "Wireless Ethernet". A brief overview of the differences between 802.11a, b, and g are as describes as follows:

802.11a. This standard describes operation in the 5GHz band and uses OFDM thereby enabling raw transmission rates up to 54 Mbps. Some countries have other uses (air traffic control and military) defined for this band so it is therefore not globally accepted to be used in ISM applications. In some cases it can be used inside buildings with limited power. In the U.S., the 5GHz band is treated as the other 900MHz and 2.4GHz ISM bands. One advantage of IEEE 802.11a is that it operates with the same data rates (54 Mbps) as IEEE 802.11g but escapes the sometimes crowded 2.4GHz channels. Less interference in the 5GHz band means the potential for more reliable transmission.

802.11b. This standard, adopted in 1999 uses the 2.4GHz band with DSSS modulation. The raw transmission rate is limited to 11 Mbps.

802.11g. This standard adopted the OFDM technology of 802.11a in the globally accepted 2.4GHz band. Using the OFDM technique over the air data rates can be increased to 54 Mbps. Its important to note that 802.11g is backwards compatible with 802.11b and given its increased over the air data rate capability will likely replace 802.11b as price points are expected to lower in the future.

Figure 3 below summarizes the above differences between the different IEEE 802.11a/b/g variants. Which one is the best for a given application, depends on common application issues as speed requirements, 2.4GHz traffic, interoperability with other equipment, and sometimes distance.

	802.11a	*802.11b*	*802.11g*
Frequency	5.8GHz	2.4GHz	2.4GHz
Distance *	Shortest	Longest	Long
Speed	54Mbps	11Mbps	54Mbps
Compatibility	802.11a	802.11b	Backwards to 802.11b
Usage	Least	Most	Replacing 802.11b for speed
Pros	Unaffected by 2.4GHz traffic and can co-exist with 2.4GHz networks. Channels have no overlap.	Very large user base. Long distance with a low cost.	Higher speed than 802.11b using same bandwidth.
Cons	High cable/free space loss at 5.8GHz yields 70% distance of 2.4GHz with same cables and antennas.	Relatively low network speed. DSSS has high multi-path latency. Channels overlap.	Low energy per bit, shorter distance than 802.11b at same frequency. Channels overlap.

* Distance comparison is general based on all installation parameters being equal. Actual performance depends on antenna type, system attenuation, and line of site issues.

Figure 3 – Comparison of IEEE 802.11a/b/g

Security / Encryption Explained.

With wired communication a physical electrical connection is used for the transmission medium which means that a physical connection, or at least physically close inductive coupling, is required to intercept the signal. Because wireless communication uses an open and shared medium (the air) anyone can technically receive a signal or message after it is transmitted. The sometimes ease of reception of wireless signals is therefore the technical reason security concerns are often a barrier to wireless adoption in industrial applications. When public standard technology such as that based on IEEE 802.11 standards is used this concern is sometimes greater since the standard for which the technology is based is public information.

Wireless technology has been the target for many different types of attacks for many years. These attacks are diverse in scale and reasoning from trying to collect personal information to causing harm in an infrastructure resulting in network downtime potential costing companies hundreds of thousands of dollars in lost productivity. Because of this the need to protect the wireless network and the information that is transmitted on it is essential. In the public 802.11 standard there are several

different levels of security, or encryption as it is referred to, that has evolved over time. When the 802.11a/b subsets where first ratified the IEEE struggled with what level of encryption should be required to comply with the standard. WEP or Wired Equivalency Privacy was settled upon. WEP provided the same level of security to the wireless network that was provided by a wired Ethernet network. This level of encryption did not serve as a good level of security in the wireless standard because inherently wireless systems are less secure then wired systems. This variability of the security was prayed upon by wireless attackers. Today this level of encryption is so susceptible to wireless attacks that even the most novice computer user can find the tools online that will allow access to any WEP encrypted network. Therefore a higher level of security needed to be developed. WPA or Wi-Fi Protected Access was introduced to meet this need.

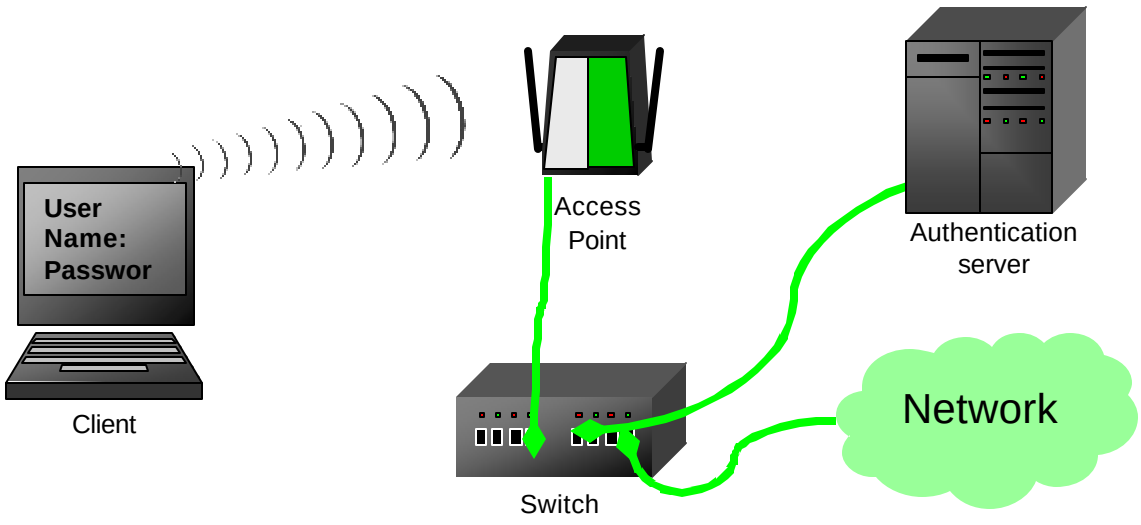
WPA is based on the same type of encryption that is used in WEP although advancements where made providing for more secure communications. Two major advancements that WPA provides over WEP are authentication and dynamic keys. The authentication process was added to help restrict rouge client (wireless end devices) access. There are two levels of this authentication PSK (Pre-Shared Key) which is generally used in SOHO (Small Office Home Office) networks where only a low level of security is required. The higher level of authentication security is 802.1x this is a standard that was developed by the IEEE to provide secure communication between the client device and authentication server such as a RADIUS (Remote Authentication Dial In User Service). This server is responsible for verifying client devices and allowing access to the network. This level of authentication is generally used in enterprise networks. Dynamic keys are also a large factor in the security of a wireless network. Keys are the component of a wireless system that encrypts the information being sent. To communicate on a wireless network the key much be known by the client device. A wireless network is considered breached or hacked when an undesired client device gains access to the network which means the key has be found or cracked. One way to keep the network secure is to continuously change the key that is used this is done by using TKIP (Temporal Key Integrity Protocol) which creates dynamic keys or keys that are constantly changing. Overall WPA is a good form of security it provides a high level of protection from many different types of wireless attacks. Although WPA security is still vulnerable to more sophisticated wireless attackers. This is due to the fact that the encryption is based on the pervious WEP standard. Because of this, if a completely secure network is required WPA and WEP are not the suitable security standards. The IEEE committees recognized this problem and developed a new security standard IEEE 802.11i also known as WPA2.

The new standard WPA2 uses a completely new form of encryption called AES (Advanced Encryption Standard). AES was previously used by the government as a replacement for the DES (Data Encryption Standard) to protect all of the government's wirelessly transmitted information. This new high level of encryption is considered "un-hackable" by many security experts today. The term un-hackable is defined as keeping unauthorized users off the network eliminating their ability to cause harm to the infrastructure and retrieve sensitive information that the wireless system may be communicating. The new WPA2 security also maintains a high level of authentication by employing 802.1x to communicate to an authentication server providing the most secure form of wireless communication. WPA2 offers more then just the highest level of security and allows for pre-authentication.

Encryption Method	Description	Security
WEP	Weak key can be hacked or cracked with little to no security knowledge	Poor
WPA	Based on the same encryption as WEP with added features like authentication. Can be hacked although it takes more time and a higher knowledge of network security	Good
WPA2	Currently the highest level of security available and is considered un-hackable by today's standards.	Best

Figure 4 – Encryption Comparisons

Pre-authentication allows a client device the ability to connect with one access point while becoming authenticated with another. This allows the client to roam from access point to access point seamlessly and will not loss a wireless connection. An example of this would be a laptop being used to monitor network status wirelessly as the laptop is moved around the factory away from one access point towards another the laptop will detect that the signal from the one access point is becoming weaker and the signal from another access point is becoming greater. Rather then the laptop continuing to loss signal strength and slow speed it will switch access points to maintain the best wireless connection. Older security standards like WEP and WPA will allow the wireless signal to become weaker and speed will slow until the network is unusable. Then after losing a connection the laptop will search and reconnect to the network using another access point. This will cause a loss of a network connection and a delay in getting information. Overall WPA2 is currently the best security that can be used to protect wirelessly transmitted information combining an "un-hackable" encryption with the security from 802.1x authentication and a seamless wireless connection with pre-authentication.



- Client tries to join the network
- Using specific port defined by 802.1x the EAP (Extensible Authentication Protocol) is used to talk to the Authentication Server
  - Because of the 802.1x port protocol nothing can see the authentication process and the client can see nothing on the network
- Handshaking occurs and the Authentication server ether authorized or denied access to the client

Figure 5 - Example of 802.1x Authentication Procedure

Industrial Requirements

It is generally accepted that limitations on data throughput, performance, and RF behavior mean wireless Ethernet based on IEEE 802.11 technology is not yet capable of the determinism required for critical process control applications. However, the ability to increase data access via WLANs, provide Ethernet TCP/IP access to remote installations, and bridge networks enables some exciting application possibilities within the industrial space. However, as is often the case industrial applications typically require special hardware and software considerations. On the hardware side of things environmental concerns are typically the most important. Products that are packaged for use in control cabinets or that have IP 67 ratings so they can be mounted stand-alone in the tough environment of the factory floor are often necessary. Additionally increased operation reliability means greater emphasis on filtering of the RF signal and immunity to EMI, RFI, and even influences of lightning then what might be required of an office environment equivalent. The RF environment in an industrial application is also additionally challenged by a phenomenon called multi-path. This is the effect when radio waves strike a very dense object such as metal or stone and are reflected similar to the way a mirror reflects light. Some of the reflected waves will be received by the receiving antenna at different times then the intended signal and therefore out of phase. This effect can seriously degrade, and in some cases,

completely cancel the received signal. Since the industrial landscape is typically crowded with large metal structures multi-path interference is especially problematic. The solution to multi-path problems found on industrial solutions is usually described as antenna diversity. Two antenna ports are provided on the receiving unit and an internal circuit selects the antenna that receives the stronger signal.

Another issue regarding industrial use of the IEEE 802.11 is the suitability of the physical and software interface to the industrial application. Solutions need to meet application and interface requirements of both the controls engineer as well as the most involved IT department. As an example, new products on the market allow a control engineer to use an Ethernet radio to address remote I/O via add on modules that can be easily addressed via XML or MODBUS TCP/IP. Since many serial devices still exist in industrial applications its also helpful to have serial gateway functionality as an example to convert MODBUS RTU data (serial port) to MODBUS TCP/IP over the air for network access. Support of Power over Ethernet (PoE) can also be a valuable feature when remote access points are installed. This allows power to be provided to the Ethernet radio via the network cabling. Finally, since many industrial installations have greater physical area to cover then common commercial applications its possible to get industrial solutions with higher power (up to 400mW) and high gain antennas have also proved to be very effective in extending distance.

Industrial Applications

Many industrial plants and facilities have increased their productivity, security, and network communications capabilities via Industrial Wi-Fi (IEEE 802.11) technology. Listed below are just a few examples of these applications.

Mobile Computing (Industrial "Hot Spot"). What is becoming a common application for mobile computing is to support workforce management data applications. Basically a "hot-spot" is created using an industrial IEEE 802.11 product as an access point. Mobile clients, in this example the laptop or pocket PC of a utility or water / wastewater maintenance personnel, can then roam into a covered zone and access their work orders and service orders from their trucks saving valuable time and scarce office resources. With proper firewalls and using a high level security encryption (described above) this application can also provide remote access to SCADA applications.

Video Surveillance. With ever increasing concern and attention about plant security perimeter monitoring and video surveillance have become very important subjects. Recent technological advances in camera technology mean IP access can be provided very easily. The IP camera typically includes embedded set up and control software making access possible from any PC. However, you still have to run expensive data cabling, sometimes to remote areas of your facility. Wireless Ethernet based on IEEE 802.11 technology can provide more then enough bandwidth to stream video. This many times allows fast and easy installations with relatively minimal cost. Also, when combined with an industrial Ethernet radio that has addressable I/O an application such as gate monitoring and access control can be accomplished with very little design and installation effort.

Network Bridging / Remote Access. It's often required to bridge two Ethernet networks, as an example when connecting the networks of two buildings located physically apart from each other.

In the case of many industrial applications, it is important to gain network access to remotely located devices via a wireless bridge. An example of this might be an electric generation facility or wastewater treatment facility with remotely located pumps. These pumps are often controlled by Ethernet accessible VFDs (variable frequency drives). Great operational benefit can be achieved by communication to the pumps from the control room network. Trenching and running cable for this could easily approach tens of thousands of dollars; therefore making the project cost prohibitive. Industrial Ethernet radio devices set up as a bridge can easily connect the remotely located asset to the rest of the plant network providing greater monitoring and control capabilities.

Conclusion

Although "Wi-Fi" technology has a certain connotation of commercial technology, with appropriate security features, industrial hardware, and industrial interface products based on IEEE 802.11 technology are becoming viable solutions for many industrial communication and networking applications.