IEEE 802.11 for Industrial Applications

Wireless networking is catching the attention of a lot of people these days. Its impact is growing and spreading out from its early focus on office network applications into a host of other areas. In the industrial data communications space wireless local area networks (WLANs) are attracting attention in a similar way that wired Ethernet LANs did, albeit more quickly. Once Ethernet technology became commonplace, reliable and affordable, the industrial market started looking at it more seriously, considering how it could meet the unique and often stringent requirements of industrial applications.

Of course, proprietary wireless systems (point-to-point and networked) have been around for a while, but cost, lack of standardization and performance limitations have been an impediment to their range of implementation. As the cost/performance ratio of IEEE 802.11 wireless (or Wi-Fi) has improved, manufacturers and users have begun to develop products and systems specifically for industrial applications.

Now users are looking to WLANs for solutions to a wider range of needs. Inexpensive, reliable wireless networks allow industrial users to enhance data collection, human-machine interfaces (HMI) and web-based system monitoring, programming and management. The ability to implement new projects without the time and expense of running cables is a compelling proposition. Maintenance departments can readily see the value in providing mobile access for updating, reprogramming and re-calibrating equipment over a wireless network.

Basics of the IEEE 802.11 Standard

IEEE 802.11 is a set of standards (first introduced in 1997) that defines how multiple devices can communicate on a wireless network. The standard has grown into a set of several standards with alphabetical suffixes that (as of this writing) extend from a to v. The standard defines the physical and data link layers only. As a part of the IEEE family of standards, it is not surprising that 802.11 WLANs are easily connected to 802.3 (Ethernet) LANs. Higher layer LAN protocols, network operating systems and internetworking protocols such as TCP/IP integrate seamlessly.

Under the IEEE 802.11 standard there can be two different types of devices on the network: stations and access points. For wireless office networks a station is usually a desktop PC equipped with a wireless network interface card (NIC) or a portable computer with built in Wi-Fi or a PCMCIA Wi-Fi card added. For industrial applications the range of possibilities is wider. For example, a station could be a Wi-Fi enabled PDA (personal digital assistant) used as an HMI. Another possibility is an 802.11 wireless serial server connected directly to a programmable logic controller (PLC), HMI, or other field device.

An 802.11 access point is a radio with an interface that allows connection to a wired LAN. Access points run bridging software (specified by 802.11d) to facilitate the connection from wireless to wired network. The access point becomes the base station for the WLAN. It aggregates access to the wired network for multiple wireless stations. An access point could be a standalone device or a card in a PC.

Wireless Network Configurations

The 802.11 standard defines two modes of operation: infrastructure mode and ad hoc mode. Infrastructure mode makes use of one or more access points connected to a wired LAN. Wireless stations communicate with access points to gain access to each other and/or the LAN. In the Basic Service Set (BSS) several stations communicate with one access point, which is connected to a wired LAN. In the Extended Service Set (ESS) two or more access points connect to the LAN creating a subnetwork.

In ad hoc mode, also called Independent Basic Service Set (IBSS), access points are not used. Wireless stations communicate directly with each other in a peer-to-peer fashion. This mode allows individual computers to set up a network where wireless infrastructure does not exist.

The original physical layer specification of 802.11 defined a WLAN operating in the 2.4 GHz ISM band, which does not require FCC licensing. Three different options were specified: two using spread-spectrum radio and one using infrared. The infrared option never gained much traction. The radio options operate at 1 Mbps and 2 Mbps using frequency hopping spread spectrum (FHSS) or direct sequence spread spectrum (DSSS) techniques. The two techniques are not interoperable and provide different performance characteristics. Frequency hopping has the advantage of providing better noise immunity but limits the top end data rate.

802.11b Raises the Bar

Networks based on the original 802.11 had the advantage of being based on a widely accepted standard, as opposed to earlier proprietary networks. But it quickly became clear that data rates of 1 to 2 Mbps were inadequate, especially when the goal was often to interconnect with Ethernet LANs that operated at 10 Mbps (10Base-T) and later 100 Mbps (100Base-TX). The 802.11b standard was the first attempt to address these data rate limitations. The result was a standard that, like the original specification, utilizes the 2.4 GHz band, but achieves data rates as high as 11 Mbps, bringing it into the same range as 10BaseT.

IEEE 802.11b implements the same DSSS modulation scheme used for one mode of 802.11, but dropped the FHSS mode because of inherent data rate limitations. Although FHSS provided superior noise immunity for 802.11, the newer standard compensates by incorporating several other modulation and coding schemes that ensure good noise immunity. One of these is dynamic rate shifting, which causes it to fallback to lower data rates to compensate for higher noise levels.

IEEE 802.11g Steps Up

IEEE 802.11g takes a big step forward without cutting ties to its siblings. The standard specifies a WLAN that operates on the 2.4 GHz band at data rates as high as 54 Mbps, but is backward compatible with the earlier standard. It incorporates at least two modes of operation, one that is compatible with the slower 802.11b and another that operates at the higher data rate. Systems can incorporate 802.11b and 802.11g equipment and they will interoperate. However, when connected into the same network the 802.11g equipment will operate at the 11 Mbps limitation of the 802.11b equipment. To overcome this problem separate b and g networks can be created and linked together through a router or access point (if it is equipped with the necessary capabilities). This keeps slower 802.11b traffic separate and allows the 802.11g WLAN to operate at the higher data rate.

IEEE 802.11a an Alternative

Another member of the 802.11 family—the 802.11a version—takes a slightly different approach by operating in the 5 GHz band. Like the 2.4 GHz band, 5 GHz does not require licensing and has the added advantage of being less congested. The maximum data rate for 802.11a is 54 Mbps, the same as for 802.11g. While 802.11a WLANs have some advantages, the downside is that they are not directly compatible with the b and g versions. In order to connect 802.11a to either of the other networks special bridging equipment must be used.

The 802.11 Data Link Layer

Like 802.3 (Ethernet), the 802.11 data link layer is made up of two sub-layers: the Logical Link Control (LLC) sub-layer and the Media Access Control (MAC) sub-layer. Both 802.3 and 802.11 use the same LLC, specified by 802.2, one reason why integrating 802.11 and 802.3 networks is relatively simple. The 802.11 MAC sub-layer is also similar but does different in the way the shared radio carrier is accessed. While Ethernet uses Carrier Sense Multiple Access with Collision Detection (CSMA/CD), 802.11 uses a variation called Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA).

In CSMA/CA a station that intends to transmit 'listens' for traffic on the radio carrier frequency and sends if it is clear after a random delay period. If the receiving station receives the packet intact it sends an acknowledgement (ACK) to confirm the packet has been received. If the transmitting station does not receive an ACK it assumes a collision occurred and transmits again after a random delay period.

Another aspect of the 802.11 data link layer that is different than Ethernet is the use of a packet fragmentation and CRC error checking with each packet. Ethernet implements these functions at higher protocol layers whereas 802.11 fragments packets and uses CRC at the data link layer. This allows the WLAN to send smaller packets that are less likely to be corrupted by interference, decreasing the need for re-transmissions.

802.11 Range, Security and Other Considerations

IEEE 802.11 devices communicate via radio signals that must penetrate solid objects to reach other network nodes. These signals are attenuated to varying degrees depending on the type of material and its thickness. The transmitter power output, the type of antenna used and the amount of attenuation through materials affects the useable range. Other factors also affect range and overall performance. Electromagnetic noise, the amount of network traffic, other radio devices operating in the same frequency band (e.g. portable phones, etc) and reflections (multipathing) are factors. In an infrastructure network the number of access points and their coverage pattern also affect how well the system operates. Typically an 802.11 device operating indoors will have a range from 100 feet minimum to about 500 feet maximum. Outdoors, some products, using high gain antennae may achieve line-of-sight ranges of five miles or more.

Security is a significant concern for WLAN users, and industrial users are not exempt. Whether security threats originate intentionally or unintentionally, wireless systems are more susceptible than wired systems. IEEE 802.11b uses Wired Equivalent Privacy (WEP) protocol to encrypt transmitted data. Designed to provide the same level of security as that of a wired LAN, WEP operates at the physical and data link layers of the network and has been found to be somewhat lacking. IEEE 802.11g originally implemented a more robust security standard called Wi-Fi Protected Access (WPA), a scheme designed to improve on WEP's limitations. It has better encryption algorithms and uses a technique called authentication. WPA was considered an interim standard. IEEE's 802.11i standard (which was adopted recently) incorporates WPA as well as additional security features. It is expected to replace WPA.

Industrial Applications Challenge WLANs

Applying WLANs to industrial applications presents added challenges compared with home or enterprise applications. Industrial environments often produce significant amounts of electrical noise. Variable frequency drives, competing radio systems, radar and microwave sources and welders are a few examples of industrial noise sources. Signal attenuation and reflections also can compromise signal coverage in industrial buildings and worksites. Transmitter power levels, receiver sensitivity and access point placement is critical. Reliability of individual components and the

overall system can affect plant safety, security and downtime costs. Industrial users demand performance guarantees. These guarantees extend to system characteristics such as data latency and corruption levels.

In response, many manufacturers are marketing equipment designed to address these challenges. For example, stations and access points targeting the industrial market implement higher transmitter power levels. Industrially focused equipment increasingly offers weatherproof enclosures, industrial mounting options and connectors and other robust features. Manufacturers often include software to perform RF site surveys to assess the consistency and reliability of plant coverage. Some access points include remote management software.

The list of 802.11 modems, serial servers, repeaters, access points and other equipment grows daily. Quality and ruggedness continues to improve. At the same time the 802.11 standard continues to evolve while maintaining backward compatibility. Industrial equipment manufacturers and users are embracing wireless networking in concept and practice, and finding success in the process. IEEE 802.11 compliant WLANs are a key part of that trend.