Skyway's wireless jump

by William J Miller, MaCT

The Holcim(US) Chicago Skyway slag cement plant will serve as the site of a second pilot test of the latest wireless mesh communication system called Wave Relay™ which is designed for the demanding industrial environment. The first pilot test, conducted in June of 2002, demonstrated the advantages of multi-hopping wireless technology in typical plant configurations. This report explains the role secure wireless ad hoc networking for process controls, using the Holcim case study as an example of the feasibility of this technology within an infrastructure system in a harsh industrial environment.

A general lack of network infrastructure throughout the plant and surrounding areas, as well as the effects of the industrial environment on wireless signal propagation made multi-hop communication an appealing solution. The test also provided an opportunity to understand the range of environmental conditions that can be expected in an industrial plant such as dust, extreme temperature ranges, and operation during intermittent power conditions such as electrical storms. As sensor actuator and mesh communication networks mature, they will play a primary role in industrial process control systems. Often industrial facilities span a large geographic area making traditional wired Ethernet connectivity both difficult and expensive to deploy. Wireless communication systems provide an ideal solution for many industrial process control tasks.

The role of wireless communication in industrial facilities

- Remote monitoring of plant operations. Plant operators will be able to monitor and control the plant while remaining completely mobile. Operators will no longer be confined to the control room.
- Sensor devices will be able to continuously monitor plant equipment and notify operators if specific conditions occur.
- Programmable Logic Controllers (PLC's) will link in with the plant network wirelessly. This allows easy reorganization of systems which occurs frequently in assembly lines.
- Remote plant facilities will be able to connect wirelessly to communicate with the plant control system. This occurs frequently in water treatment plants where water towers are located across a large geographic area, but are monitored from a centralised location.
- The wireless communication infrastructure can be used for video surveillance throughout the plant facility. Workers will also rely on wireless technologies for voice communication.

Holcim (US) Chicago Skyway facility

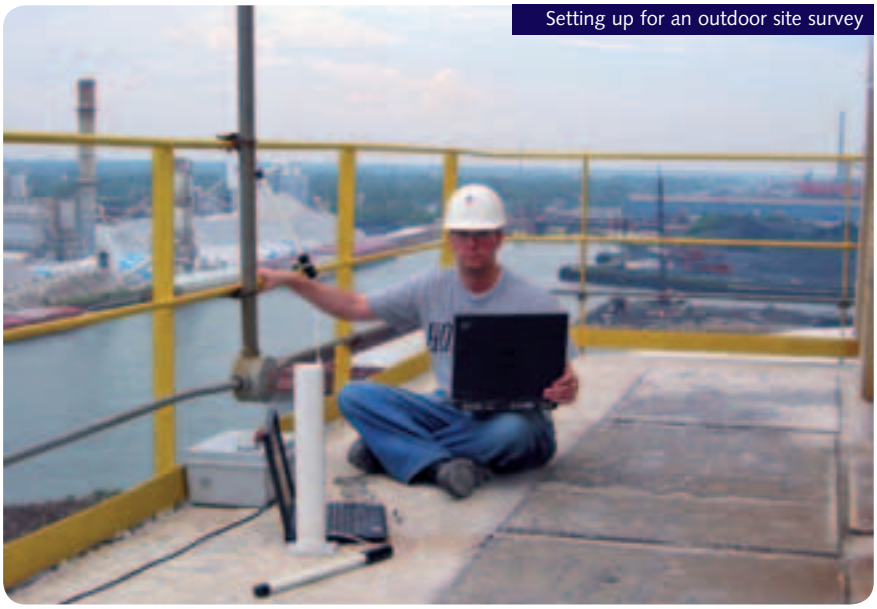
Critical infrastructure protection

Industrial process control systems are responsible for maintaining the nation's power grid and water supply and as such require extremely high security and network availability. If an attacker was able to gain access to industrial control system software remotely over a wireless network the consequences could be devastating. In addition, the latency requirements of the control loop present unique demands on wireless communication protocols.

In the past, networks have strongly relied on physical security. The concept of a network firewall is a perfect example in this direction. A network firewall is intended to provide an access control division between the insecure public network (the Internet) and the seemingly secure private internal network.

However, the rapid adoption of wireless networking technology makes the assumption about the physical security of the network infrastructure unrealistic. This is because the wireless shared medium is completely exposed to outsiders and susceptible to attacks that could potentially target any of the OSI/ISO layers in the network stack. Examples of such attacks include jamming of the physical layer, disruption of the medium access control layer coordination packets, attacks against the routing infrastructure, targeted attacks on the transport protocols (such as an attack against packets addressed to a specific port), or even attacks intended to disrupt specific applications.

In addition to the vulnerabilities of the



Setting up for an outdoor site survey

wireless communication infrastructure, the ultra portability of modern devices provides an increased susceptibility to theft. Over the past year, 59 per cent of companies surveyed in the CSI/FBI Computer Crime and Security Survey reported that laptops had been stolen. The cost of these stolen devices is minimal in comparison to the information they contain and the resources they provide access to. If an attacker was able to use a stolen device to gain access to the control system of an industrial plant, the result could be catastrophic.

RF Propagation

The physical characteristics of industrial plants present a number of challenges to wireless system deployment. The interior of industrial plants are often covered by metal. The walls are made of sheet metal, the machines are made of metal, and the floor is a grated metal. This makes RF communication extremely challenging. We also found that most industrial facilities have minimal wired network connectivity.

Traditional Ethernet cable is impractical due to long cable lengths and powerful low frequency interference from machinery. Expensive fiber optic solutions are required. In many of our experiments, the only available access to Ethernet was in the control rooms. This lack of existing wired infrastructure makes deploying access points difficult. However, we were able to deploy a multi-hop ad hoc network to provide connectivity throughout the plant.

Throughput and loss rate measurements fluctuated dramatically as the test devices were moved throughout the plant. The

environment experienced massive multi-path effects as the wireless signal bounced off all of the metal surfaces. Technologies such as MIMO (Multiple-Input-Multiple-Output) will play an important role in these types of environments. These multi-path effects make it extremely difficult to deploy typical access point based solutions since it is almost impossible to provide total coverage. A multi-hop communication system allows routes to adapt as the communication quality fluctuates. This adaptation attempts to provide the most efficient utilisation of the wireless medium under any set of environmental conditions.

Conclusion

The pilot project allowed us to simultaneously demonstrate and prove the feasibility of a secure wireless infrastructure system in a harsh industrial environment. Even though the environment was challenging, consisting of thick cement walls, metal machinery, steel beams, and sheet metal walls, the Wave Relay™ self-configuring network was able to move data across multiple hops through the wireless network. In addition, the performance characteristics of different types of wireless adapters were able to be tested under these conditions. Our initial experiments showed that devices operating in the 2.4 GHz spectrum tended to outperform those which operated in the 5 GHz band. We also observed that multi-rate wireless devices would tend to immediately reduce their transmission rate to compensate for the multi-path characteristics within the plant. Once operating at lower speeds the devices would communicate effectively. Overall this experience was extremely useful allowing us to experiment with existing technologies in a difficult operating environment while simultaneously proving the functionality of the Wave Relay™ system under conditions that truly demand its advanced functionality.

Testing operation inside of the plant