Wireless Security for Water/Waste Water Networks

Brian Cunningham
Applications Engineer
Eaton/Cooper Bussmann, Wireless Business Unit*
Port Coquitlam, BC V3C 6G5
1-866-713-4409
www.cooperbussmann.com/wireless

Keywords

radio, mesh, wireless, network, management, systems, monitoring, spread spectrum, telemetry, frequency hopping, transmitter, receiver, transceiver, encryption, security

Abstract

Wireless technologies have been used for decades in the water/waste water industry in a multitude of applications including tank level indication, pump and motor control, flow and pressure monitoring, etc. However, recent concerns regarding the potential for hacking and cyber-attacks into these wireless systems have raised the importance of wireless security to a new high. This paper will discuss security issues within an Industrial Wireless Network, and address the ways in which these networks can be designed to be more reliable while being more secure.

1.0 Introduction

On April 23, 2000, millions of liters of raw sewage were pumped into the public waterways, parks and the grounds of a Hyatt Regency hotel in Maroochydore, Queensland Australia in what is believed to be the first successful wireless hacking attack on a public water system. Vitek Boden, a disgruntled employee of the contractor that installed the waste management system, was convicted on hacking charges and damaging the environment, and sentenced to 3 years in prison. The Maroochy Shire Council then spent another $176,000 to improve security and monitoring after the incident, during which it had hired private investigators to track Boden, ending in a police car chase in which Boden was forced off the road and arrested.

The above incident illustrates that wireless hacking of water systems can be done, and if proper security is not maintained, the network is then left open to anyone with sufficient motivation.

2.0 Wireless Systems for Water/Waste Water Applications

Before a discussion of wireless security can begin, the reasons why the wireless network is there in the first place need to be covered. Water/Waste Water (W/WW) systems generally consist of reservoirs and/or water storage tanks, piping networks and their associated pumps, and a treatment plant. For potable water, the treatment plant can be a chlorination plant, filtration plant, ultra-violet disinfection plant or any combination of methods to disinfect water. For waste water, the treatment plant is a combination of primary, secondary and/or tertiary treatment before discharge into a lake, river or ocean.

Treatment plant wireless networks have different characteristics from piping networks mainly defined by the distance. Piping networks collecting sewage and delivering potable water span every neighborhood in a city so their wireless communications have to cover great distances, and as such will require higher transmit power radios, taller antenna masts, lower frequency radios, and the use of repeaters. On the other hand, treatment plant applications are over much shorter distances, usually gathering 4-20mA and contact closures from pH sensors, chlorine sensors, etc and sending them to the control room. Treatment plant networks can utilize wireless systems with much lower transmit power and very small antennas such as WirelessHART™ or ISA100 devices.

These wireless systems have become popular for one primary reason; cost. In piping networks there are relatively few options. Leased telephone lines being the primary option, they can be expensive on a monthly basis and have reliability issues. In treatment plants, cost is the same motivation for utilizing wireless systems. Digging a trench to lay buried conduit costs money and time and in some cases requires permits.

A wireless system can be installed and commissioned by a qualified electrician in half a day depending on some of the mechanical requirements of the site.

Figure 1 – Burying Conduit

Next is the reliability concern of wireless signals. This is a more fundamental concern of if it will work, even before we discuss the potential of hackers to disrupt the system. When the spread spectrum bands were first introduced, FCC created rules to allow frequency hopping (FH) technology to be used. This meant that radios could change frequency to avoid interference. The rules also allowed a modulation technique called direct sequence (DS). Direct sequence radios can suppress interference using processing gain. More recently, FH and DS have been combined yielding the best of both worlds resulting in yet higher performance of the radio system in the presence of interference. Radio modulation schemes continue to evolve resulting in higher throughputs, greater ranges, better performance in the presence of interference and better co-existence with other nearby radio networks. We have seen this evolution not only in the SCADA world, but also in the cellular world with 2G being surpassed by 3G, and now 4G, and also in the popular 802.11 standards with 802.11b being surpassed by 802.11g, and now 802.11n. The result is more reliable, better performing wireless networks.

3.0 Reliable Radio – The Basics

With mention in the previous section of all the different modulation techniques, a short discussion on what has been found to be the most reliable, as well as techniques to make your system harder to hack is in order.

First, in general terms, FH radios have been found to be the most robust. FH technology was developed originally for military use, and is still used by militaries around the world because it is harder to jam. It constantly changes frequency, so unlike most other modulation techniques, a hacker must learn what frequencies the system will use. One small but additional step.

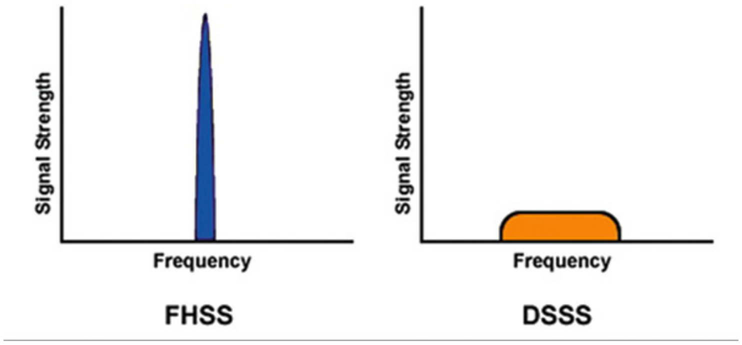

Figure 2 – Frequency Hopping vs Direct Sequence Spread Spectrum

Next the signal to noise ratio must be considered. With most radios, when the noise comes within 10dB of the signal strength, the radio will lose link because it is unable to distinguish a digital “1” or “0” from the noise. Therefore maintaining a strong radio link will make it difficult, but not impossible, for a hacker to inject a false signal, while the original transmitting radio is still trying to get a message through. A radio with higher transmit power and high gain antennas will boost the signal.

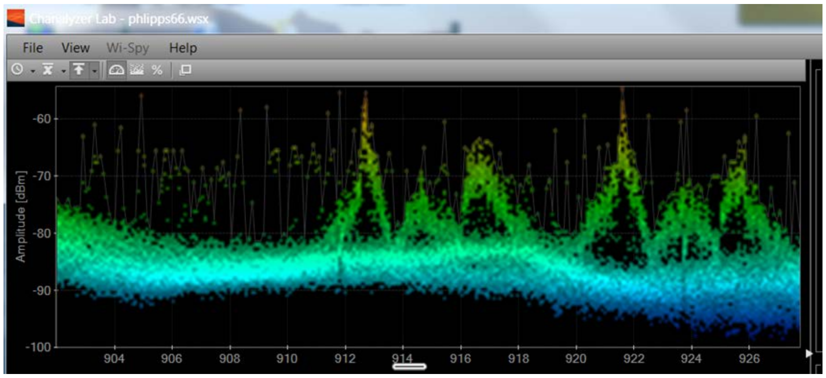

Figure 3 – Background Noise Measurement

Antennas come in 2 general styles; omni and yagi directional. If possible, use yagi directional antennas. Yagi directional antennas require aiming and can only ‘hear’ radio signals coming from the direction they are aimed in, whereas omni antennas transmit and receive over 360 degrees. Thus, if a hacker wants to inject false signals, he will need to be in the path of the yagi antenna. However, if this is a repeater or base station location, then often there is little choice but to use an omni antenna.

3.0 Protocols – Public or Proprietary?

Many users wish to utilize public wireless protocols so that equipment from one manufacturer can communicate with that of another. 802.11a/b/g is one example of a public protocol enabling, for example, a laptop made by Dell to communicate with a wireless router made by D-Link. The protocol format is in the public domain, available to anyone.

On the other hand, many manufacturers of wireless equipment have produced their own proprietary protocols that are optimized for a specific application. The benefits of this are reduced overhead, allowing more throughput for actual user data. As an example, with 802.11, approximately half of the bandwidth is used up as overhead to allow it to be used in many varied applications. Most proprietary wireless protocols will reduce that down to 25% or less, of the bandwidth being used for overhead.

Proprietary protocols may not be that difficult to hack, however it adds an additional step that must be done before a hacking attack is successful. If it’s being done wirelessly, it means being parked in a vehicle onsite longer, to gather enough messages to interpret the protocol which may raise suspicions.

4.0 Encryption Techniques

There are many different encryption techniques available to wireless manufacturers. Encryption is intended to hide the meaning of the message. How successful it is depends on if, and then how long it takes to decrypt the messages. There are many different encryption schemes available and following is a short summary of the most popular ones. Note that this paper is not intended to be an analysis of cryptography, which is a field of study unto its own.

Prior to a few notes on encryption, it’s important not to forget about physical security. Proper locks, fences, and monitoring of entrance doors and cabinet doors will let you know if someone has physically breached a facility – bypassing your wireless security. Policies on user rights, passwords and when they should be changed will go a long ways towards securing a network. RADUIS servers that provide centralized authentication, and virtual LAN’s to segregate process data from the public domain should also be considered.

WEP – Wired Equivalency Privacy is an encryption technique used by many 802.11 wireless networks. It is available as a 64 bit or 128 bit key, usually entered as 10 or 26 hexadecimal characters. This key is then concatenated (added) to a randomly generated initialization vector. This keystream is then XORed with the plain text forming the encrypted message. For a client device to be authenticated with an Access Point, two methods can be used, Open System and Shared Key. In Open System, data is just sent, and if decrypted using the correct key, the data is passed. In Shared Key, the WEP key is used in a four step challenge – response handshake, whereby a non-encrypted message is replied to with encryption, and if successful, the client becomes authenticated (passed the encryption test) and associated (established a connection with the Access Point). Open System is in fact more secure, since it is possible to derive the key from the handshake process – though both systems are considered weak.

Many freeware programs today exist to crack WEP encryption keys. As a result, it is not considered a secure encryption technique, but included with many wireless systems for legacy compatibility.

WPA - Wi-Fi Protected Access is a security encryption method that supersedes WEP. WPA includes TKIP (Temporal Key Integrity Protocol). The previous WEP standard used fixed keys that do not change. TKIP dynamically generates a new 128-bit key for each packet and thus prevents the types of hacking that allowed WEP encryption to be compromised. WPA also includes a Message Integrity Check (MIC). This prevents a hacker from resending data packets or possibly altering them and then resending preventing spoofing attacks.

WPA2 – also known as 802.11i, makes use of the Advanced Encryption Standard (AES) where as WEP and WPA used the older and less secure RC4 cipher. It also uses CCMP instead of TKIP used by WPA. CCMP (Counter Cipher Mode Protocol) is considered even more secure than TKIP.

AES – Advanced Encryption Standard replaced an older encryption scheme called DES. It is considered secure enough, that when used with longer key lengths of 192 or 256 bits, suitable for TOP SECRET data within the US Government.

As shown above, encryption techniques have evolved as the field has advanced with computers with more processing power and attacks revealing weaknesses becoming public knowledge. Overall, for long term security, it would seem to be a poor choice to use a public wireless standard such as 802.11x if alternatives are available.

5.0 Conclusion

Wireless networks in the W/WW industry offer significant cost savings and operational flexibility, which has led to their wide scale deployment. Each installation must be designed for maximum reliability, before trust can be placed on its operation. Consideration of modulation technique, frequencies, signal-to-noise ratios and antenna selection can make a system more reliable as well as more difficult to hack. Proprietary wireless protocols will put an additional barrier up that a hacker must overcome but lock a network into a single manufacturer. Encryption of wireless data is mandatory for security, however as processing power of computers increase and encryption weaknesses publically revealed, it would be best not to combine 802.11 frequencies with a public encryption technique for long term use. Lastly, as Vitek Boden proved, wireless attacks on W/WW networks can occur and if proper security is not implemented, the public cannot count on a reliable and safe potable water supply, and sewage to be treated and disposed of as intended.

www.cooperbussmann.com/wireless
www.eaton.com/wireless

Technical Support:
United States: +1 866 713 4409
Australia: +61 7 3352 8624

Email: ELPRO-Support@cooperindustries.com
ELPRO-US-Support@cooperindustries.comm

Note: Eaton acquired Cooper Industries plc in November 2012