Wireless Networking for International Safeguards

Susan Caskey, Heidi Anne Smartt, Don Glidewell, Jason Coombs
Sandia National Laboratories
Masato Hori, Yu Hashimoto
Japan Nuclear Cycle Development Institute (JNC)

Abstract:
Wireless networking using the IEEE 802.11standards is a viable alternative for data communications in safeguards applications. This paper discusses the range of 802.11-based networking applications, along with their advantages and disadvantages. For maximum performance, safety, and security, Wireless networking should be implemented only after a comprehensive site survey has determined detailed requirements, hazards, and threats.

1. Introduction

While wireless networking was not originally designed for use in industrial applications, or within a nuclear facility, there is potential for its use in safeguard applications. Wireless networking can offer more freedom in sensor placements and reduce costs associated with cable installations. The IEEE 802.11 wireless specification allows any IP data to be transmitted transparently to sending or receiving devices. IEEE 802.11 systems are commercially available from a wide variety of vendors and, with proper installation and security measures, can be as secure as hardwire networking.

The most common wireless networking methods include third-generation mobile telephony networks (3G), Bluetooth, and IEEE 802.11 (wireless Ethernet). The standardization of 3G has not been fully ratified, and the capability of 3G varies depending on location. It can theoretically support transmissions at 2 million bits per second (Mbps), but the most recent versions have sustained data rates of only 50 to 60 thousand bits per second (Kbps), and rates under 20Kbps are common. Bluetooth is an industry standard for use in connecting small system peripherals. The typical maximum distance for Bluetooth transmissions is 10m or less, and data rates of 1Mbps are available. IEEE 802.11 is a standard for wireless transmission of Internet protocol (IP) data. Unlike 3G and Bluetooth, it is currently widely used in commercial network installations. Since neither 3G nor Bluetooth directly support IP data transmissions, IEEE 802.11 is the most likely candidate for nuclear safeguards today. The Experimental Reactor Joyo facility is currently looking at wireless solutions for transmitting data between a number of areas both within containment and outside. A wireless site survey was preformed at this facility to determine the possible locations of 802.11 wireless systems and the feasibility of their use.

2. Wireless Network Security

With any networking technology, the potential for compromise of the data and of the network itself is a common threat and must be addressed.

In 802.11 networks, unlike wired networks, physical security does not prohibit unauthorized access to the network. The nature of radio allows anyone with a receiving device within the range of the transmitter to detect the transmission. Such eavesdropping does not require any special device to

detect or sniff the data transmissions as they are passed between units. In fact, a number of programs available on the Internet allow an individual with a wireless card to intercept the data packets and reconstruct an entire wireless session. These are very similar to the packet sniffers used on wired networks.

WEP is a built in 802.11encryption protocol designed to prohibit network sniffing. However, there is a core flaw in the implementation of WEP that allows its encryption key to be cracked. A 128-bit WEP key can be cracked in as few as 4 million captured packets, which on a busy network can take less than an hour. WEP uses the RC4 algorithm, which itself is a strong algorithm. However, the implementation of RC4 in WEP allows the key to be discovered because the initialization vector is repeated every 2^{24} bits. Software programs like AirSnort[i] (The Schmoo Group, 2003) gather the data packets, decipher the key, and produce the decrypted information automatically. WEPCrack[ii] is another tool that deciphers the WEP key using the weakness of RC4 key scheduling. Both of these software packages are free and simple to use.

2.2 Attack Vectors

A number of active attacks against 802.11 networks are common to both wireless networks and wired networks, the most common being man-in-the-middle and denial-of-service (DOS) attacks.

Man-in-the-middle attacks involve an attacker sniffing packets from a network, modifying them, and inserting them back into the network without being detected. A rogue access point (or multiple rogue access points) can be used to intercept packets and pass them along to the actual destination. These rogue access points are made to look valid, so the wireless units associate with them and transmit the data packets to the rogue access points instead of the legitimate access point. Other risks exist for an attacker to flood the network with a copy of past traffic (a replay attack), which can be used to disguise the attacker's data, flood the network, or cause systems to transmit more reset data, allowing for faster WEP key deciphering.

DOS attacks can be mounted against the wireless network itself or against the radio portion. Attacks against the network include flooding the IP network with data, which reduces the ability to transmit legitimate data. Repeatedly spoofing disassociation packets and forcing a unit to re-associate before transmission can begin also disables all transmissions from the unit. Radio based DOS attacks use a device running at the same frequency as the wireless network and flooding all the channels with noise. Radio DOS can also be caused accidentally by introducing new radio devices into the network vicinity. However, the use of spread-spectrum technology reduces both incidental interference and active radio jamming.

2.3 Security Solutions

There are solutions to most of the weaknesses of 802.11, and the IEEE has developed a working group, 802.11i, to examine and institute enhancements. The most serious weakness in 802.11 is the authentication of both the transmitting and the receiving units. With a robust authentication scheme, man-in-the-middle and network DOS attacks become far more difficult.

Partially to provide this authentication functionality, the IEEE ratified the 802.1x standard for port-based network access control. It was originally designed for wired technologies like Ethernet, but is a viable option for access control of 802.11 systems, and many of the high-end 802.11 devices fully support 802.1x. Authentication under 802.1x uses a multi-stage process to allow connection from a client unit to the access point. The client unit first associates with the access point but is placed in a holding network segment until the unit has been authenticated. This holding segment can be configured to allow limited access or no access on the wired network. The access point requests identification from the client unit, and the client responds with a user name or other specific identifier. The access point forwards the identifier using the wired link to an authentication system like a RADIUS server. The RADIUS server transmits a challenge to the client unit and the client responds. No password or key is ever transmitted over the wireless link. Once the RADIUS server has verified authentication of the client unit, and the client has authenticated the identity of the network through the RADIUS server, the access point grants the client full access to the network.

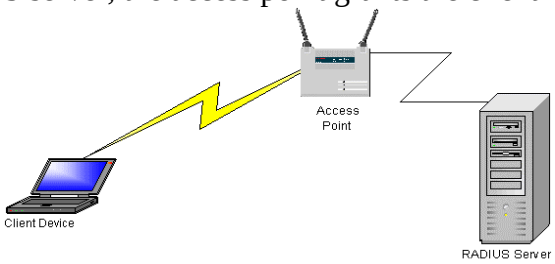

Fig. 1. *802.1x Authentication*

2.4 Alternatives to WEP

To address the weakness of WEP for data encryption, Cisco developed a protocol called Temporal Key Integrity Protocol (TKIP) that was later adopted by IEEE. TKIP is a near-term solution to the deficiencies of the 802.11 implementation of RC4. TKIP is not yet a fully ratified standard, but is in use by a number of 802.11 vendors. TKIP uses a 48-bit key versus the 24-bit key of WEP. It also encrypts the portion of the header that contains the sending and receiving address; any alteration to this information caused by interception would be detectible. The next version of TKIP will likely migrate from the RC4 algorithm to AES for data transmission, but since the overhead with AES is slightly larger then RC4, RC4 may still be used for header information.

Virtual private networks (VPNs) can also be used over the wireless network to solve a number of the security issues independently of the 802.11 standard. A VPN/firewall can be installed to run on each side of the wireless connection to provide network authentication, in-transit data protection, and protection against man-in-the-middle attacks. VPN is a relatively mature technology and has already been introduced into many networks. VPNs offer a wide range of encryption algorithms including AES and 3DES, and they interoperate with other matching VPN devices. The VPN/firewall would provide all network security and allow the wireless devices to work without WEP, which has the added benefit of increasing throughput of the wireless network.

Fig. 2. *VPN Authentication/Encryption on Wireless Network*

3. 802.11 Physical Layer

The 802.11 standard offers a wide variety of radio configuration options to account for the wide variety of deployment characteristics. The type of data to be transmitted over the wireless network and the requirements of the data will help determine which of the current 802.11 options will offer the best performance. The 802.11b standard is the slowest at 11Mbps, but it offers the greatest number of hardware options. The newest standard, 802.11g, runs at 54Mbps and is also backward compatible with 802.11b. The first standard ratified, 802.11a, was the last to be implemented. It also runs at 54Mbps. If bandwidth is critical, either the 'a' or the 'g' option should be used. Both 'b' and 'g' transmit at 2.4 GHz and can span 11 channels, of which only 3 are non-overlapping. 802.11a transmits at the 5.2GHz band and can utilize 8 non-overlapping channels.

4. Safeguards Applications

Studies of wireless networking within industrial applications have been inconclusive as to its functionality, but most of the recent studies have shown that 802.11 wireless systems can provide the functionality required to transmit safeguards information. Networking systems using 802.11b have been successfully deployed in US nuclear sites for the transmission of voice and video data. When deploying wireless networking technology within a nuclear facility, extra care and deliberate advance planning are critical. The hardware used must be proven and secure and must be carefully characterized in terms of performance, thermal and other energy output, redundancy, and configuration.

The transmission of safeguards information is typically not high in bandwidth, but tends to contain bursts of data, which may include imagery and text-based information. The low-bandwidth data requirements of safeguards information allow for a reduction of radio signal strength and may allow for different deployment strategies. The frequencies allowed within each country may limit which systems can be used and how the power settings for each system can or cannot be modified. In general, the 2.4GHz frequency band is less governed worldwide than other RF bands. Nevertheless, each facility must be evaluated specifically to determine if and where wireless networking will be of benefit. Depending on the location of the various wireless systems, there is potential of attenuation too great for the data transmissions to be received. However, radio transmissions can propagate through some materials and can be installed in crawl spaces and other unexamined airways.

In addition to a single area, wireless networking can also be used for building-to-building communications. Building-to-building communications may allow for monitoring of facilities that currently do not have access any external network infrastructure. The 802.11 MAC specification of CSMA/CA requires a specific timing of data to handle data retransmissions. The default 802.11 specifications and the speed of light allow for multi-network systems with no distances greater than 15km. However, in a point-to-point deployment, this distance can be increased to 30km or even 50km by modifying the default system settings.

For most safeguards installations, there will not be a large number of wireless systems moving from access point to access point. Therefore, the use of a VPN/firewall to provide the necessary protection of the network and data is likely the best choice for deployment. Within an installation where there are ever-changing devices, a system like 802.1x may be more useful.

5. JOYO Wireless Site Survey

The Experimental Reactor Joyo is currently evaluating communication options for the upgrade of the IAEA's DMOS system and is also investigating communication options for data transmission within the entire campus area, specifically to allow the extension of the JNC's external network into areas which currently only allow internal JNC network access. The facility is currently using PHS (personal handy-phone system) cell phones in all areas for voice communication and has installed extra cellular antennas within most areas. PHS cell phones use the TDMA (time division multiple access) technology and are able to transmit with a data rate close to 128Kbps. These systems could allow a limited amount of data to be transmitted short term, but do to the limited bandwidth of the current PHS systems these would not be a viable long-term solution.

To provide information about other wireless networking options, a wireless site survey of was performed within the reactor area using 802.11b systems running at the 2.4GHz frequency. The systems used for the survey were a Cisco 350 Access Point, a Cisco 350 Work Group Bridge, a Netgear WLAN card and a Prisim WLAN card. The antennas used on both the access point and the wireless bridge were standard 4 inch "rubber duck" antennas. Also an Arintsu spectrum analyzer was used to verify possible interferences before the tests were started. The test was to determine possible wireless network transmissions between the Fresh Fuel Storage area (FFS1), the Spent Fuel area #1 (SFP1), the Cask Car area, and the reactor core.

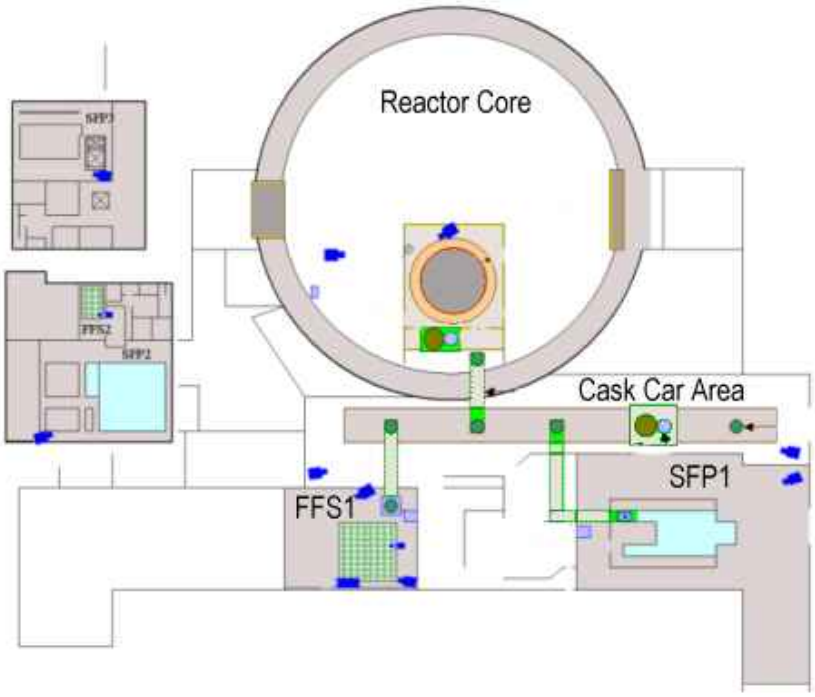

***Fig. 3**. Joyo Reactor Facility*

The Arintsu RF spectrum analyzer measures radio waves between 100MHz and 3GHz in frequency. For the first phase of the survey, this unit was used to listen to radio signals within FFS1, the Cask Car Area, and the reactor core. There was very little RF traffic seen in these areas, except for a small increase of less then ½ a db centering at 1.9GHz and spanning less then 500MHz. As the PHS cell phones run at this frequency, this was the likely cause of this signal. There was a single instance of a signal spanning from 1.9GHz to 3Ghz or higher. This signal was only seen once and for a duration of under 20sec. Since this signal was not seen again, it was a possible false reading of the analyzer.

The next phase of the test was to transmit information between two systems using the 802.11b devices. Initially, the access point was installed in the hallway near the fresh fuel storage area. (Fig. 4) The bridge and both WLAN's were able to connect both within the FFS1 and along the entire cask car area. The radio signal strength from the wireless bridge located inside FFS1 was at 60-80% and allowed an average data rate of 175 Kbps. A WLAN card also located inside FFS1 had a signal strength of 20%, but still allowed data transmission rates similar to that of the bridge unit.

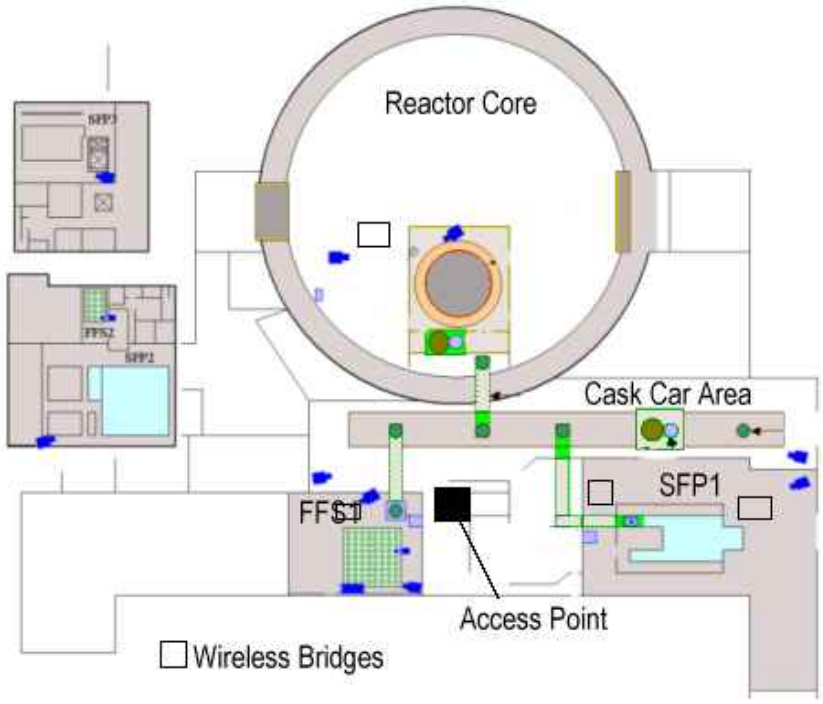

***Fig. 4**. Access Point located in Cask Car Area*

The wireless bridge and a WLAN system were then moved into SFP1 where initially neither were able to connect. However, after a minor location change, a connection was made to the access point still located in the cask car area near FFS1. It was discovered that a door between SFP1 and the cask car area was propped open to allow for some construction. With this door closed, the WLAN card was unable to connect. The wireless bridge was still able to maintain a signal at 70-80% strength with the door open or closed. The data rate between the bridge and the access point averaged 196 Kbps.

A direct wireless connection was not possible from FFS1 to SFP1, but an access point in the cask car area solved this problem by bridging the two areas. The wireless bridge unit was then moved into the reactor core while the access point remained in the cask car area. As expected, no wireless connection could penetrate the reactor shielding. However, wireless transmissions within the core were possible. All systems were able to transmit at full strength with a data rate topping at 11 Mbps.

The wireless survey showed that wireless networking using the 802.11 systems at 2.4GHz is a possible solution to allow data transmission within FFS1, SFP1, and the cask car area. Using a standard hardware Ethernet connection via a twisted pair connection or other cable already installed, wireless units can be installed within the core and within the cask car area to allow wireless networking within the entire reactor area. The data rates calculated would allow multiple data transmissions and allow for all types of IP data.

6. Conclusion

Wireless networking using the 802.11 specification will provide more flexibility and less cost of installation for safeguards applications than traditional wired networks. No single option is best suited for all installations, but with proper analysis of the site, a wireless solution specific for the installation can be determined. Security must be a key element in the design phase, but with the appropriate protective measures, a wireless network could provide convenient and cost effective networking within a nuclear facility where a wired network might not be feasible.

Bibilography

Gast, Matthew S., *802.11 Wireless Networks, the definitive guide*. O'Reilly and Associates, USA. 2002.
Reidn, Neil and Seide, Ron, *802.11 (Wi-Fi) Networking Handbook.* McGraw-Hill/Osborne, USA. 2003
Gier, Jim, *Beating Signal Loss in WLANs*. http://80211-planet.com/tutorials/articles.php/1431101.
--, *Understanding Wireless LAN Bridges.* http://80211-planet.com/tutorials/articles.php/1563991.
--, *802.11a Physical Layer Revealed*. http://80211-planet.com/tutorials/articles.php/2109881.
--, *802.11 MAC Layer Defined*. http://80211-planet.com/tutorials/articles.php/1216351.
--, *802.11b Physical Layer Revealed*. http://80211-planet.com/tutorials/articles.php/2107261.
--, *Infrared WLAN*. http://80211-planet.com/tutorials/articles.php/2110301.
LAN's Unplugged: Wireless LANs and IEEE 802.11.
http://www.networkmagazine.com/article/PIT20000410S0047/2.
Everyone's Wireless, *Wireless Technology FAQ*. http://www.everyones-wireless.com/tech_faq.htm.
OFDM Tutorial. http://www.wave-report.com/tutorials/OFDM.htm.
Peck, Martin R., *Wireless Attacks and Exploits*. http://cubicmetercrystal.com/janus/attacks.html.
Fluhrer, Scott; Mantin, Itsik; and Shamir, Adi, *Weaknesses in the Key Scheduling Algorithm or RC4*, http://www.drizzle.com/~aboba/IEEE/rc4_ksaproc.pdf.
Cisilion, *Advantages of Wireless Networking*, http://www.cisilion.com/wireless_advantages.htm.

References

---

i The Schmoo Group, *Airsnort HomePage*. http://airsnort.shmoo.com
ii Project WEPCrack, *Project: WepCrack: Summary,* http://sourceforge.net/projects/wepcrack.