Honeywell

THE POWER OF **CONNECTED**

Wireless Network Security and Data Reliability

A Technical Note

Background

Wireless technology is becoming a popular choice for automating various types of industrial processes and applications. The benefits and advantages of wireless technology include:

- Enhanced worker safety. Wireless technology enables a worker not to be physically present in a potentially hazardous location whenever she or he needs to take instrument reading or monitor systems.
- Simplified connectivity. Thanks to wireless systems, there is typically no need to setup conduits, trenches, dedicated power supplies, or junction boxes.
- Increased flexibility. Wireless technology allows for the easy deployment of additional wireless sensors and enables expansion of an existing wireless network with relative ease.
- Improved overall maintenance and servicing of the instruments and system.

As companies become more and more digital, network security also becomes a top priority. Wireless network security becomes increasingly important when a third-party Ethernet device such as a Wireless Ethernet Gateway is physically connected to a Programmable Logic Controller (PLC) or Distributed Control System (DCS) that controls and aggregates data for system automation. With inadequate network security protocols, malicious software and/or malware could infiltrate a wireless gateway and thereby gain access to an organization's information networks, servers, and databases. Manufacturers of industrial wireless products understand the threat of malicious cyber activity and the need for security protocols to be embedded or certified in all wireless products.

Introduction

Traditionally, industrial facilities such as factories, process industries, petro-chemical plants, and oil & gas refineries have used wired systems for process applications. Today, wireless technology can be easily and cost effectively retro-fitted into different applications and systems such as pressure monitoring in oil rigs, refinery process control, tank level monitoring, and overhead door detection in warehouses. As industrial facilities install industrial wireless technology, data reliability and wireless network security are two application elements that must be taken seriously.

For more information on ODVA's vision for securing the flow of data in industrial networks, visit: https://www.odva.org/Portals/0/Library/Publications_Numbered/PUB00278R2_Optimization-of-Industrial-Cybersecurity.pdf

Most sensors that have been wired for control and monitoring applications can be equipped with a wireless chip that can have one or multiple wireless protocols. These wireless protocols can be Bluetooth® Low Energy (BLE), Radio Frequency (RF), ZigBee®, ISA100 Wireless™, Wireless HART, Cellular etc. System integrators should be aware of the potential risks if the signal from the sensors is not reliable, so highly sophisticated and secure firewalls, data encryption, and anti-virus systems are installed to help mitigate the risks from various internet-based hardwired protocols as well wireless protocols.

Similarly, data reliability can also create issues and uncertainties during system automation and control if the sensor data is not consistently making its way to the wireless receivers or gateways. As an example, consider a wireless pressure sensor used to monitor the level of a petroleum product in a tank. The sensor data is being used for automating a process application. If the signal quality between the wireless sensor and the wireless receiver is not reliable, the sensor data may not reach the receiver. When the liquid in the tank is getting low and the warning signal is not received, the workers would not have enough time to switch to another tank or refill the tank they were currently using for the process application. This unplanned downtime could have financial implications if the worker has to completely stop the process application or any delay in the process may cause quality issues in the final petroleum product.

ODVA is a global association whose mission is to advance open, interoperable information and communication technologies in industrial automation. ODVA has recommended a defense-in-depth, multi-layer approach to help protect against cyber-attacks on industrial control systems. ODVA offers a variety of tests

Honeywell's Wireless Technology

The communication protocol used in Honeywell's Limitless Wireless products is based on the internationally accepted IEEE 802.15.4 Standard for Low-Rate Wireless Networks. Honeywell uses the 2.4 GHz Industrial, Scientific and Medical (ISM) radio band and the Direct Sequence Spread Spectrum (DSSS) frequency modulation technique for data transmission and reception. The 2.4 GHz ISM radio band is license free worldwide. It is possible to transmit large data packets at a higher rate and has a high resistance to the interferences created by other wireless sources. This standard has been in place for a number of years with several generations of devices already deployed.

The IEEE 802.15.4 protocol and interconnection for data communication devices using low-data-rate, low-power, and low-complexity short-range radio-frequency (RF) transmissions in a wireless personal area network (WPAN) specifications include:

- Improved Medium Access Control (MAC) layer security,
- Channel agility eliminates crosstalk with other wireless networks,
- Prioritized channel access resists interference from out-of-network users in the same frequency band such as Bluetooth, Wi-Fi and portable phones.

Source: "IEEE Standard for Low-Rate Wireless Networks" by IEEE Computer Society, 2015, Copyright © 2016 by The Institute of Electrical and Electronics Engineers, Inc.

All of Honeywell's wireless products are designed with features that mitigate the risk of wireless network security concerns and helps ensure that 100% of the sensor data makes its way to the receiver.

For complete product information including datasheets, CAD models, installation instructions and up-to-date distributor inventory, visit https://sensing.honeywell.com/wireless

HONEYWELL LIMITLESS WIRELESS PORTFOLIO			
Pressure Sensors	 WPS	 IS-WPS	 IS-WPS ISA100
Limit Switches	 WLS	 WGLA	 WBX
 WBX ISA100	 WLS-EP	 WLS-SSA	 WLS-RS
Operator Interface	 WOI		
Receivers	 WMPR	 WDRR	 WPMM

Wireless Network Security

The DSSS method is a spread-spectrum modulation technique for RF communication system where the transmitted RF data is multiplied with a pseudo-random code. DSSS randomly generates a mathematical key called Pseudo Random Code (PRN) that which is then multiplied with the RF signal.

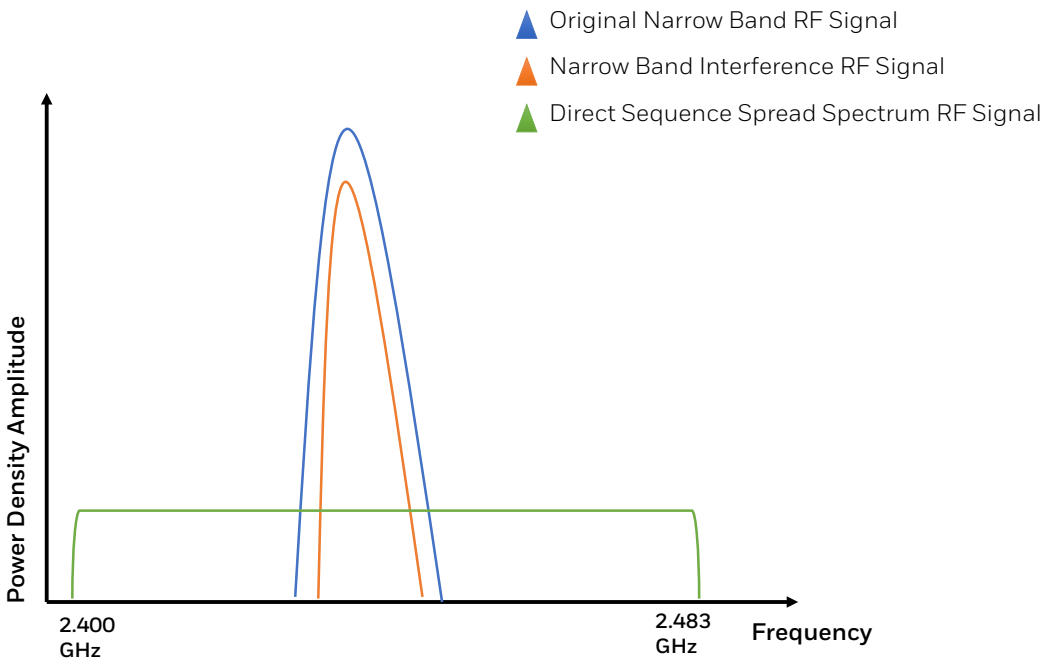
In the DSSS technique, the RF data packet is spread across the entire range of frequencies available in the RF bandwidth before transmission. Honeywell's wireless products use 16 frequency channels within the 2.4GHz bandwidth. Then, the spread RF signal is multiplied with a randomly generated Pseudo Random Code or Chipping Code. The encrypted RF signal is then transmitted into the air. The transmitted wideband RF data packet also has the decoding key with the help of which the receiver decodes the data packet.

At the receiver end, the received wideband RF signal is again spread throughout the entire 16 frequency channels. The decoding key is then re-applied to each data bit of the received RF signal. With the help of the super-imposed decoding key, the receiver decodes the encrypted RF signal back to its original form. The wideband RF signal is narrowed down to its original format and the narrowband RF interferences picked up during the air transmission is decoded to a low power density signal which is either eliminated or ignored by the receiver.

Data Reliability

The IEEE 802.15.4 specification provides higher resistance to RF interferences. Honeywell's wireless products use 16 frequency channels within the 2.4 GHz band and utilizes the direct sequence spread spectrum (DSSS) frequency modulation. The DSSS frequency modulation uses a redundant bit pattern feature so that an alternate or duplicate copy of each transmitted data bit exist in the transmitted wideband RF signal. This characteristic helps ensures 100% data reception at the receiver end and also increases the signal resistance to RF interferences and other environmental noises. DSSS frequency modulation technique uses low-power density for RF signal transmission and reception as shown in Figure 1, it is harder to detect or eavesdrop the RF signal.

Figure 1 – Direct Sequence Spread Spectrum Signal Transmission



The narrow band interfering signals may have no effect, while wideband noise sources may cause loss. The effect of light-to-moderate interference is not going to make the system fail, but may increase the rate of missed data packets. The missed data packets are immediately retransmitted in millisecond time frame, hence the user may not notice any delay in data reception.

However, if the rate of missed RF signals increases, the transmitted data will take much longer to reach the receiver than normal. If this transmission delay is significant, then it can disrupt system automation programs running on a PLC or a DCS system. This time delay will only be noticeable if an application is time sensitive and if a transmitter is configured to sample and report data extremely fast such as <1 sec sample and report intervals. But if a transmitter is sampling and reporting every 30 sec, then the delay caused by any missed data packet should not be an issue.

Honeywell's wireless products have a pairing procedure that follows the security techniques outlined in IEEE 802.15.4 standard. This pairing technique ensures communication between the receiver and nodes. When registration is activated the receiver provides the nodes with several pieces of information:

1. Receiver's individual 16-bit network identification number, which the receiver randomly generates at power-up to avoid conflict with other 2.4 GHz wireless radios in the vicinity.
2. The receiver generates a unique 16-bit address for each of the nodes in its wireless network.
3. A 128-bit encryption key that the pair will use to encode future wireless communications.

The combination of addressing and encryption ensures the uniqueness and reliability of the device's communications channel. As a result, even if multiple Honeywell's wireless networks exists in the same location, the node(s) from each wireless network will only communicate with its respective wireless receiver. This feature potentially eliminates the possibility of cross-talking between Honeywell's wireless networks with any other 2.4 GHz wireless networks.

Additionally, another way to help ensure data reliability is by maintaining a radio signal strength between a wireless receiver and its respective nodes in the highest category. Honeywell's wireless products have a site survey or radio signal strength indication (RSSI) feature that allows an end user to determine the radio signal strength between two wireless devices. It is highly recommended to perform a site survey before installing a Honeywell wireless system. The site survey feature can be initiated from the wireless receiver. If the wireless receiver is equipped with LCD display, the display will indicate the radio signal strength (see Figure 2). If the site survey result is not up to the recommended optimal status or Excellent/Very Good/Good category, then it is recommended to use higher-gain antennas on either the transmitter, the receiver, or on both the devices and perform another site survey to verify the RSSI. Only after a satisfactory site survey, install the products in their final destinations.

Figure 2 - Radio Signal Strength Indication Screenshot of WMPR Wireless Receiver

Summary

As wireless technology becomes a popular choice for automating various types of industrial processes and applications, network security also becomes a top priority.

The MAC layer of WPAN IEEE 802.15.4 wireless standard uses the 128-bit symmetric-key cryptography technique that increases data confidentiality and significantly reduces eavesdropping and eliminates cross-talking with other 2.4 GHz wireless networks. The Direct Sequence Spread Spectrum RF modulation technique utilizes the Pseudo Random Code (PRN) to enhance data security. The redundant bit pattern characteristic of DSSS helps ensure that 100% of the transmitted data is received at the receiver end. It is for these reasons, Honeywell uses this technology in all of our Limitless wireless products.

Warranty/Remedy

Honeywell warrants goods of its manufacture as being free of defective materials and faulty workmanship during the applicable warranty period. Honeywell's standard product warranty applies unless agreed to otherwise by Honeywell in writing; please refer to your order acknowledgment or consult your local sales office for specific warranty details. If warranted goods are returned to Honeywell during the period of coverage, Honeywell will repair or replace, at its option, without charge those items that Honeywell, in its sole discretion, finds defective. **The foregoing is buyer's sole remedy and is in lieu of all other warranties, expressed or implied, including those of merchantability and fitness for a particular purpose. In no event shall Honeywell be liable for consequential, special, or indirect damages.**

While Honeywell may provide application assistance personally, through our literature and the Honeywell web site, it is buyer's sole responsibility to determine the suitability of the product in the application.

Specifications may change without notice. The information we supply is believed to be accurate and reliable as of this writing. However, Honeywell assumes no responsibility for its use.

For more information

To learn more about Honeywell Limitless wireless sensors and switches, call 1-800-537-6945 or visit sensing.honeywell.com/wireless

Honeywell Sensing and Internet of Things

9680 Old Bailes Road
Fort Mill, SC 29707
honeywell.com

002421-1-EN | 1 | 09/17

Honeywell