Wireless Sensor Networking for the Industrial Internet of Things

Joy Weiss, Vice President, IoT Security & Solutions, Analog Devices
Ross Yu, Product Marketing Manager, SmartMesh® Products, Analog Devices

Much is being made of the Industrial Internet of Things (IoT) and the associated need for wireless connectivity for industrial sensors. But the networking needs of industrial devices and applications are distinct from the consumer world, with reliability and security high on the list. This white paper highlights some of the key network requirements specific to industrial wireless sensor networks.

The advent of low power processors, intelligent wireless networks and low power sensors coupled with "big data analytics" have led to the booming interest in the Industrial Internet of Things (IoT). Put simply, this combination of technologies enables a multitude of sensors to be put *anywhere*: not just where communications and power infrastructure exists, but anywhere there is valuable information to be gleaned about how, where or what a "thing" is. The concept of instrumenting "things" such as machines, pumps, pipelines, and rail cars with sensors is not new to the industrial world. Purpose-built sensors and networks already proliferate in industrial settings ranging from oil refineries to manufacturing lines. Historically, these operations technology (OT) systems have operated as separate networks, maintaining a high bar for network reliability and security that simply cannot be met with consumer technology. These high bar requirements filter the available technologies down to those best suited for business-critical Industrial IoT applications. In particular, the way these sensors are networked determines whether the sensors can be safely, securely and cost-effectively deployed in the harsh environments typical of industrial applications. This white paper examines some of the key requirements that distinguish industrial wireless sensor networks (WSN).

Figure 1. Sensors Anywhere—Low Power Wireless Sensor Nodes Powered Perpetually by Harvested Energy, Such as This Thermal-Harvested Wireless Temperature Sensor from ABB, Can Be Placed Optimally to Gain Additional Data in an Industrial Setting

Reliability and Security Come First

Unlike consumer applications, where cost is often the most important system attribute, industrial applications typically rate reliability and security at the top of the list. In *ON World's* global survey of industrial WSN users, reliability and security are the two most important concerns cited.[1] This is not surprising if you consider that a company's profitability, the quality and efficiency with which they produce goods and worker safety often rely on these networks. This is why reliability and security are essential for industrial wireless sensor networks.

One general principle in designing a network for *reliability* is redundancy, where failover mechanisms for likely problems enable systems to recover without data loss. In a wireless sensor network, there are two basic opportunities to harness this redundancy. First is the concept of spatial redundancy, where every wireless node has at least two other nodes with which it can communicate, and a routing scheme that allows data to be relayed to either node, but still reach the intended final destination. A properly formed

1 Industrial Wireless Sensor Networks: Trends and Developments, https://www.isa.org/standards-publications/isa-publications/intech-magazine/2012/october/web-exclusive-industrial-wireless-sensor-networks/#sthash.cI3G9ze5.dpuf

mesh network—one in which every node can communicate with two or more adjacent nodes—enjoys higher reliability than a point-to-point network by automatically sending data on an alternate path if the first path is unavailable. The second level of redundancy can be achieved by using multiple channels available in the RF spectrum. The concept of channel hopping is that pairs of nodes can change channels on every transmission, thereby averting temporary issues with any given channel in the ever changing and harsh RF environment typical of industrial applications. Within the IEEE 802.15.4 2.4GHz standard, there are fifteen spread spectrum channels available for hopping, affording channel hopping systems much more resilience than non-hopping (single channel) systems. There are several wireless mesh networking standards that include this dual spatial and channel redundancy known as Time Slotted Channel Hopping (TSCH), including IEC62591 (WirelessHART) and the forthcoming IETF 6TiSCH standard.[2] These mesh networking standards, which utilize radios in the globally available unlicensed 2.4GHz spectrum, evolved out of work by Analog Devices' SmartMesh team, who pioneered the use of TSCH protocols on low power, resource constrained devices starting in 2002 with SmartMesh products.

While TSCH is an essential building block for data reliability in harsh RF environments, the creation and maintenance of the mesh network is key for continuous, problem-free multiyear operation. An industrial wireless network often must operate for many years and over its lifetime will be subject to vastly different RF challenges and data transmission requirements. Therefore, the final ingredient required for wire-like reliability is intelligent network management software that dynamically optimizes the network topology, continuously monitoring link quality to maximize throughput despite interference or changes to the RF environment.

Security is the other critical attribute of industrial wireless sensor networks. The primary goals for security within the WSN are:

Confidentiality: Data transported in the network cannot be read by anyone but the intended recipient.

Integrity: Any message received is confirmed to be exactly the message that was sent, without additions, deletions or modifications of the content.

Authenticity: A message that claims to be from a given source is, in fact, from that source. If time is used as part of the authentication scheme, authenticity also protects a message from being recorded and replayed.

The critical security technologies that must be incorporated into a WSN to address these goals include strong encryption (e.g., AES128) with robust keys and key management, cryptographic-quality random number generators to deter replay attacks, message integrity checks (MIC) in each message, and access control lists (ACL) to explicitly permit or deny access to specific devices. These state-of-the-art wireless security technologies may be readily incorporated in many of the devices used in today's WSNs, but not all WSN products and protocols incorporate all measures.[3] Note that connecting a secure WSN to an insecure gateway is another point of vulnerability, and end-to-end security must be considered in system design.

Industrial IoT Is Not Installed by Wireless Experts

For the most part, established industries are adding Industrial IoT products and services to their legacy products, and their customers are deploying in environments with a mix of old and new equipment. The intelligence embodied in industrial WSN must confer an ease of use to Industrial IoT products that make transitions seamless to the existing field personnel. Networks should rapidly self-form so that the installer can leave the site with a stable running network, avoid service interruptions by repairing themselves when connections are weak or lost, self-report and diagnose when service interruptions do occur, and avoid costly onsite visits by requiring little or no maintenance once deployed. For many applications, their success relies in part on being deployable in areas that are difficult or dangerous to reach, so the IoT devices must operate on batteries, typically for more than five years.

Also, systems should be available for global deployment, since the widespread adoption of Industrial IoT by end users is often company wide, and requires multisite standardization. Fortunately, international industry radio standards that comprehend and fulfill this requirement are in place, including IEEE 802.15.4e TSCH.

Figure 2. Network Visibility—Network Management Software Provides Critical Visibility to the Health of the Wireless Network Such as in This SNAP-ON Software Utility from Emerson Process Management

Sensors Anywhere

For Industrial IoT applications, the precise placement of a sensor or control point is critical. Wireless technology offers the promise of no-wires communication, but if you need to power a wireless node by plugging it in, or recharge it every few hours or even months, the cost and impracticality of deployment become prohibitive. For example, adding sensors to rotating equipment to monitor conditions while the equipment is in service is not possible with wires, but the knowledge gained from in-service monitoring can allow customers to predictively maintain this critical equipment, thereby avoiding unwanted and expensive downtime.

To ensure flexible and cost-effective deployments, every node in an industrial WSN should be capable of running on batteries for at least five years, as this offers users the ultimate flexibility in coverage for Industrial IoT applications. As an example of an industrial TSCH-based WSN, Analog Devices' SmartMesh products typically operate at well under 50µA, making it very feasible to operate for many years on 2 AA batteries. In environments where there is a good source of harvested energy, it is possible to run nodes perpetually on energy harvesting (see Figure 1).

2 6TiSCH Wireless Industrial Networks: Determinism Meets IPv6: Maria Rita Palattella[1], Pascal Thubert[2], Xavier Vilajosana[3,4], Thomas Watteyne[4,5], Qin Wang[4,6], and Thomas Engel[1] Published in: Communications Magazine, IEEE (Volume: 52, Issue: 12).

3 Secure Wireless Sensor Networks Against Attacks, Kristofer Pister and Jonathan Simon, http://electronicdesign.com/communications/secure-wireless-sensor-networks-against-attacks

Time Matters

Industrial monitoring and control networks are business critical. They underpin the systems that affect the basic cost of producing goods, and the timeliness of data is essential. In the past decade, deterministic TSCH-based WSN systems have been field proven in a wide range of monitoring and control applications. These time-slotted systems, such as WirelessHART, provide time-stamped, time-bounded data transmission. In these networks, nodes that require more opportunities to send data are automatically provisioned with more time slots, and low latency transmission through the network can be achieved through the provision of multiple time slots on successive paths in the network. This coordination of data transmission also dramatically improves the ability to deploy dense networks with frequent transmissions. Without a time schedule, non-TSCH wireless networks will collapse from the uncoordinated flood of radio traffic.

Additionally, every packet in a TSCH network contains an accurate time stamp indicating the time it was sent, and network-wide time is also available at each node to coordinate control signals across a network of WSN nodes if required. The availability of time-stamped data enables data to be properly sequenced by the application even if it is received out of order, which can be helpful in diagnosing precise cause and effect in industrial applications where information from multiple sensors must be reconciled.

Visibility to Network Operation Is Key

Industrial networks are required to run continuously for many years, yet no matter how robust a network is, problems can still occur. The quality of a network that works well at installation may be affected by a variety of environmental factors during its operating life. Early and appropriate alerts to such issues are an important aspect of any industrial network, and the ability to quickly diagnose and remedy issues is key for quality of service. Not all wireless sensor networks are created equal when it comes to providing visibility to network management metrics. At a minimum, an industrial wireless network management system should provide visibility to:

- Wireless link quality, measured in signal strength (RSSI).
- End-to-end packet success rate.
- Mesh quality, highlighting nodes that do not have sufficient alternate routes to maintain a reliable network.
- Node status and battery life (where applicable).

In the best industrial implementations, intelligent networks will remediate such issues by automatically rerouting data on alternate paths, while continuously upgrading the network topology to maximize connectivity (see Figure 2).

Smart Things Deserve Smart Networks

There is considerable focus on putting more and more intelligence into things, but this is not the only place where “smarts” belong in an Industrial IoT application. Industrial IoT networks should employ intelligent end nodes and network and security management features that mirror the best that enterprise IT and OT has to offer. Networks should be highly configurable to adapt to specific application needs. Given the low power requirements to achieve long battery life, self-knowledge of network power availability and intelligent routing to maximize network-wide power consumption should be employed. Additionally, the network should automatically adapt to changes in the RF environment that might favor a dynamic change in topology. Analog Devices’ SmartMesh Network Manager not only provides network security, management and routing optimization, but it also allows users to reprogram nodes over the air if required, providing an upgrade path for future features as customer needs evolve.

The Internet of Things is very much an industrial phenomenon, with clear business drivers and compelling ROI. In these business-critical applications, industrial wireless sensor networks must meet a high bar for smarts, security and reliable wire-free operation over many years. These stringent requirements can be met with existing and emerging wireless mesh networks standards, which will be key Industrial IoT building blocks to help industrial customers transform their businesses and services in the Industrial IoT era (see Figure 3).

Figure 3. Driving Change—Software Analytics, Such as the Brains.App Software from IntelliSense.io, Use the Data from Industrial Wireless Sensor Networks to Streamline Plant Operations, Optimize Yield and Improve Safety

LT 1117 REV A • PRINTED IN USA