INDUSTRIAL WIRELESS NETWORKS -

COMPARING THE STANDARDS

PART 1

Glenn Johnson, Editor

Today wireless instrumentation is becoming more commonplace in process plants and is a more specialised implementation of wireless sensor network (WSN) technology. In this two-part article we look at the predominant industrial wireless standards.

Wireless sensor networks (WSNs) are a relatively new technology and can be defined as a collection of distributed sensor devices, communicating wirelessly, which can be used to measure and monitor physical or environmental phenomena such as temperature, pressure, corrosion, vibration, noise and environmental emissions.

History

The development of standards for WSNs began in the 1990s, when the Institute of Electrical and Electronics Engineers (IEEE) began work on a specification for low-rate wireless personal area networks (LR-WPANs). This work was finalised in 2003, when the IEEE 802.15.4 specification[1] was released, defining the physical layer (PHY) and medium access control layer (MAC) for LR-WPANs. The specification offers low power consumption, low complexity and low cost. With a growing number of systems based on the IEEE 802.15.4 appearing since its release, it has become the de facto standard for WSNs.

The ZigBee specification[2] released in 2004 was the first full standard to appear based on IEEE 802.15.4 and defined the Network Layer and Application Layer on top of the IEEE 802.15.4 PHY and MAC layers.

A newer version of the standard was released in 2006 - IEEE 802.15.4-2006 - which addressed shortcomings in relation to information security and some bugs in the original. The ZigBee Alliance released a new version of the ZigBee standard, ZigBee-2006, which included scalability improvements but was still based on the original IEEE 802.15.4-2003 standard, and therefore the security issues had not been addressed.

In 2007, the HART Communication Foundation (now known as the FieldComm Group after its merger with the Fieldbus Foundation) released the HART Field Communication Protocol Specification, Revision 7.0[3], which included a definition of a wireless interface to field devices, referred to as WirelessHART - the first specification to be released specifically designed for process automation applications. WirelessHART offers a viable wireless alternative for the traditionally wired industrial field instrumentation by providing the ability to create self-healing and self-configuring multihop mesh networks. WirelessHART was approved by the IEC as IEC 62591 Ed. 1.0 for wireless communication in process automation[4] in March 2010.

Parallel to the development of WirelessHART, the International Society of Automation (ISA) initiated work on its own set of standards for wireless systems for industrial automation. The ISA100.11a standard was ratified in September 2009[5]. Like WirelessHART, ISA100.11a aims to provide secure and reliable wireless communication for monitoring and control applications in industrial process automation applications. An updated version was released in 2011 [11].

A third specification for wireless communication for the process automation industries, WIA-PA, was developed by the Chinese Industrial Wireless Alliance (CIWA) and accepted by the IEC in 2009 as IEC 62601[6]. The scope of WIA-PA is to provide an architecture and protocols for use in industrial monitoring, measurement and control applications; however, discussion of this standard is beyond the scope of this article, and is only mentioned for completeness.

Wireless sensor nodes

A wireless sensor device consists of a sensor that measures a physical phenomenon such as temperature or pressure, an analog-to-digital converter, a processing unit to analyse the sensor data and encapsulate it in data packets for wireless transmission. Given that the purpose of a WSN is to be 'wireless', the power unit is usually a battery. A long battery lifetime is therefore a requirement and so will normally preclude the driving of a load such as an actuator in most cases.

Wireless instrumentation

Wireless instrumentation is the result of the merging of WSN technologies with

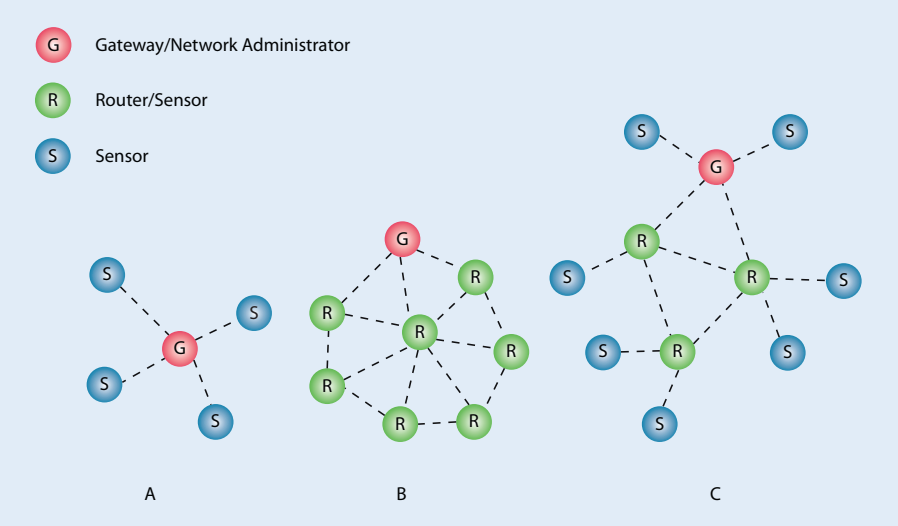

Figure 1: Examples of network topologies - A: star, B: mesh, C: hybrid star-mesh.

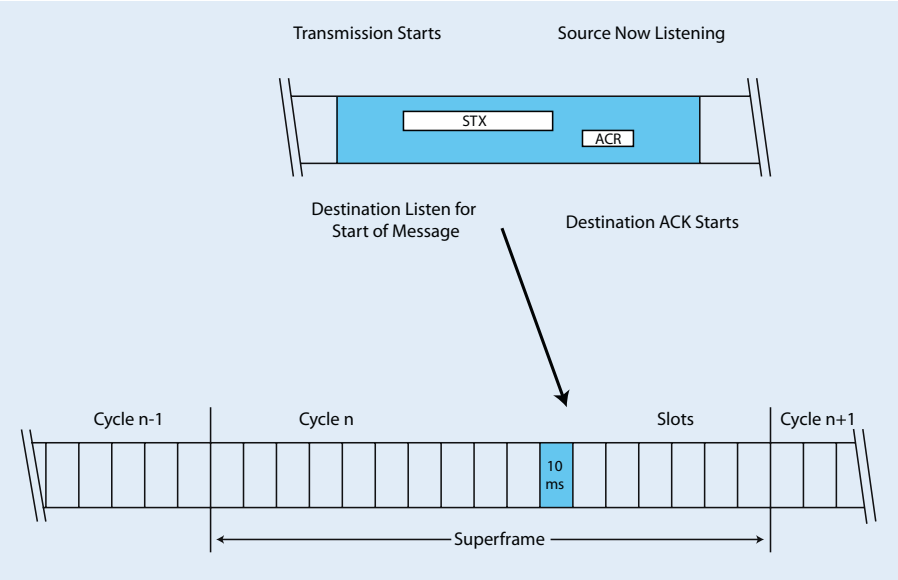

Figure 2: TDMA timeslots and superframes.

the more complex process instrumentation technology. A wireless field instrument is typically a traditional process instrument with the addition of a radio transmitter, antenna and battery. The components of the main part of the instrument itself are the same as for a wired instrument.

The performance requirements of an industrial field instrument depend on the nature and criticality of the application it is serving. This will therefore have some bearing on whether a wireless instrument is suitable in a particular application.

Network topologies

Depending on the particular implementation of the IEEE 802.15.4 network, and the capabilities of the network devices, network topologies in a WSN may range from star to a full mesh topology. In a star topology, all devices communicate with a central coordinator, as shown in Figure 1a. In this topology, the sensor devices are not capable of communicating with each other. In a mesh topology, on the other hand, all devices are capable of communicating with all other devices within radio range, creating the topology shown in Figure 1b. It is also possible to have a topology called star-mesh, in which there is a mesh network created by router devices, and an outer network of sensors connecting to the routers. An example of a star-mesh topology is shown in Figure 1c.

Routing

Routing is the process of selecting the best communication paths to deliver the data packets from source to destination, often through one or more intermediate nodes. There are two different routing algorithms which are used for routing data packets within WSNs: graph and source routing.

A graph route is a list of possible paths that connect network end nodes. A network may have multiple, overlapping graphs, offering multiple possible alternatives, and an intermediate node device may have multiple graphs going through it. The best possible route can be chosen dynamically as network conditions change.

A source route is a single directed route between source and destination nodes, defining the specific path a packet must take when travelling from its source to its destination. If any of the links in a source route fail, the packet is lost.

The routes in a network are configured by a node operating as a 'network manager', which bases its decisions based on periodic health reports from devices indicating the quality of the wireless connectivity with their neighbours.

TDMA and frequency hopping

While routing governs which radio hops are used between nodes and controls the topology dynamically, individual radio links between nodes must reliably transmit the data.

There are, of course, many factors to take into consideration in industrial environments when it comes to radio transmission. The nature of industrial environments means that there will be higher-than-average levels of interference to reliable communication, in the form of multipath fading (caused by radio reflections), electromagnetic interference and electrostatic discharge, as well as potential interference from other radio sources such as the commonly used IEEE 802.11 Wi-Fi technology. Due to the low power requirements of WSNs, these issues, as well as the security of the communication, need to be well addressed by the WSN technology. The technology also needs to provide a communication channel with at least some measure of determinacy in relation to the latency of communication. This is achieved by a combination of frequency hopping and time division multiple access (TDMA).

Time slots

With TDMA the communication is divided into distinct timeslots with a typical du-

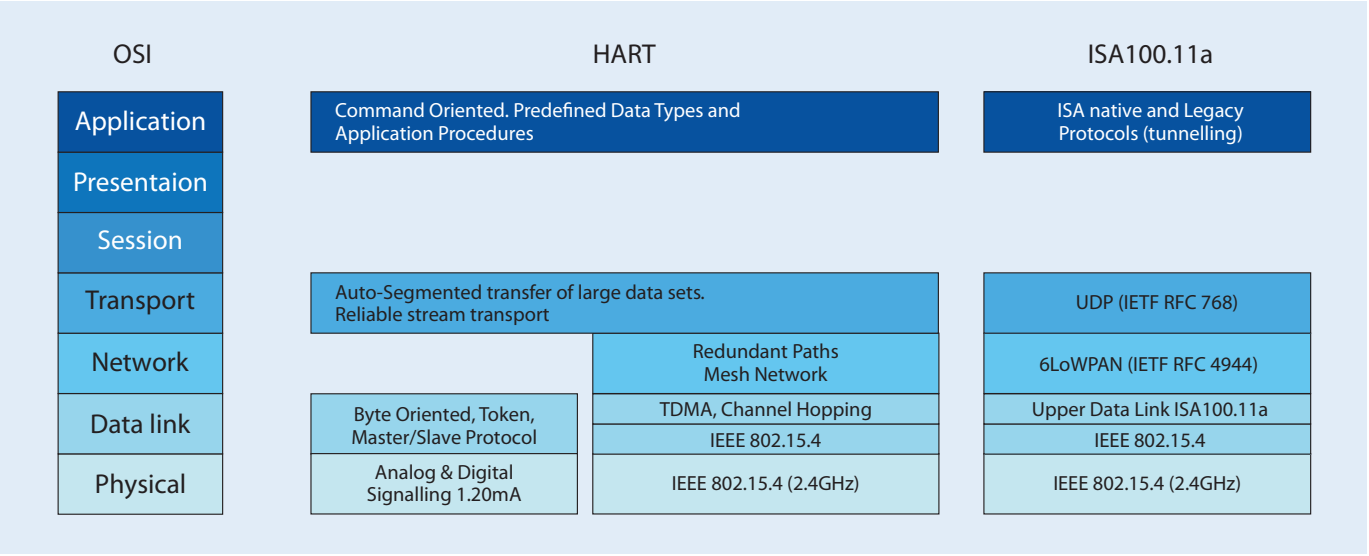

Figure 3: Industrial wireless protocol stacks.

ration of 10 ms. A collection of timeslots forms a repeating superframe. One superframe must always be enabled, although multiple superframes of variable lengths can coexist in a network.

Two devices are typically assigned to a timeslot, one as a source and the other as the destination. Broadcast messages are handled by assigning multiple devices as receivers in the same timeslot. Within a timeslot, the source device may transmit a data packet to the destination device, and on successful reception of a data packet, the destination device will transmit an acknowledgment packet (ACK) to the source device, as shown in Figure 2. If the source device fails to receive an ACK, the data packet will be retransmitted in the next available timeslot. Assigning devices to specific timeslots in a fixed length frame means that there is normally some level of fixed latency or delay between transmissions between pairs of nodes (not taking into account retransmissions).

Frequency hopping

IEEE 802.15.4 takes advantage of the licence-free 2.4 GHz ISM band, and as such may share spectrum with other licence-free radio technologies such as Wi-Fi. Like Wi-Fi, the radio band used by WSNs is divided into multiple channels. Depending on the implementation, networks may be able to switch between channels and transmit frames over different channels at different times, and also to transmit multiple frames simultaneously on different channels. The communication is therefore divided into a two-dimensional matrix consisting of TDMA timeslots and frequency channels. A link is thus specified by a superframe, a timeslot offset (relative to the first timeslot of the superframe) and a channel offset. In consecutive superframes, a link will always have the same timeslot offset, while the communication channel will change according to a pseudo-random hop sequence.

Depending on the implementation of the network, the channel selection may be fixed or may also be dependent on changing congestion or interference, choosing the appropriate channels for the most reliable communication in any given moment, much as the routing nodes can change hops as circumstances demand.

Security issues

Since WSNs have limited resources in terms of processing power and memory capacity, there are various types of security considerations and threats that need to be taken into account, such as accidental or malicious association in which a foreign device enters the network; node impersonation; man-in-the-middle attacks; denial-of-service attacks; and network injection. These issues are beyond the scope of this article, but WSN technologies need to be able to provide mitigating factors to eliminate or limit the likelihood of these events occurring, by ensuring secure communication between devices, and by providing message authenticity and data confidentiality.

International standards

As with all communication protocol standards, WSN protocol stacks can be described in terms of layers corresponding to the well-known seven-layered OSI model. Figure 3 shows HART and ISA100.11a protocol stacks in comparison. For WSNs, a simplified version of the OSI model is used, where the Presentation Layer and the Session Layer are not defined.

ZigBee

The ZigBee specification is primarily targeting smart grid, home automation and consumer electronics applications. A ZigBee network operates only on the same, user-defined channel until manually reconfigured, making it susceptible both to interference from other networks operating on the same frequency and to noise from other sources in the environment. In response to this issue, the ZigBee Alliance released the ZigBee PRO specification in 2007. ZigBee PRO is aimed at the industrial market, having enhanced security features and frequency agility so that the entire network may change its operating channel when faced with large amounts of noise or interference. Despite these improvements ZigBee has not yet been fully adopted by industry.

Another aspect of the ZigBee specification is the channel access method, CSMA (carrier sense multiple access), in which each node listens to the channel to see if it is active before sending. If a node starts sending and detects a collision, it sends a collision signal and waits a random amount of time before trying to send again. If the channel is busy, it continues to wait for an opening. Excessive traffic from a particular node, or too many nodes communicating at once, can

eventually lead to an unpredictable latency and sometimes to network unavailability. This limits the scalability of ZigBee when compared to the TDMA methods used by WirelessHART and ISA100.11.a.

6LoWPAN

6LoWPAN (IPv6 over low power wireless personal area networks) is a specification that defines the transmission of IPv6 packets on IEEE 802.15.4 networks. It is described by the IETF in RFC4919[7] and RFC4944. The 6LoWPAN definition may be used as a standalone specification for WSNs, but it is often found as an integrated part of the network layer of other specifications, such as ISA100.11a.

WirelessHART

WirelessHART enables the wireless transmission of HART messages and is based on the IEEE 802.15.4 PHY and MAC layers, although the MAC has been modified to allow for frequency hopping. TDMA with frequency hopping is used as a channel access method, and with a full mesh network topology, WirelessHART offers self-configuring and self-healing multihop communication.

ISA100.11a

In the ISA100.11a specification, TDMA with frequency hopping is also used as the channel access mechanism. ISA100.11a supports both routing and non-routing devices, so network topologies can be either star, star-mesh or full mesh depending on the configuration and capabilities of the devices in the network. It also utilises IPv6 addressing by implementing 6LoWPAN at the Network Layer.

An ISA100.11a network is able to carry multiple fieldbus protocols, such as Foundation Fieldbus and Profibus, as well as HART. There is also integrated support for IPv6 traffic and routing in the network layer.

In Part 2

In Part 2 of this article we will focus on the technical differences mainly between the two industrial wireless standards most commonly used in process automation - WirelessHART and ISA100.11a.

References

1. Institution of Electrical and Electronics Engineers, 2003, *IEEE Standard for Information Technology - Telecommunications and information exchange between systems - Local and Metropolitan networks - Specific requirements - Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low Rate Wireless Personal Area Networks (LR-WPANs)*, IEEE Computer Society.
2. ZigBee Alliance, 2004, *ZigBee Specification Version 1.0*.
3. HART Communication Foundation, 2007, *HART Field Communication Protocol Specification, Revision 7.0*.
4. International Electrotechnical Commission (IEC), 2010, *Industrial Communication Networks - Wireless Communication Network and Communication Profiles - WirelessHART*, IEC 62591.
5. International Society of Automation, 2009, *Wireless Systems for Industrial Automation: Process Control and Related Applications*, ISA100.11a-2009.
6. International Electrotechnical Commission (IEC), 2009, *Industrial Communication Networks - Fieldbus Specifications - WIA-PA Communication Network and Communication Profile*, IEC 62601.
7. Internet Engineering Task Force (IETF), 2007, *Request For Comments (RFC) 4911 - IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals*.