A Comparison of WirelessHART and ZigBee for Industrial Applications

Tomas Lennvall, Stefan Svensson
ABB Corporate Research
Forskargränd 7 SE-72178, Västerås, Sweden
{tomas.lennvall, stefan.svensson}@se.abb.com

Fredrik Hekland
ABB Corporate Research
Bergerveien 12, NO-1375, Billingstad, Norway
fredrik.hekland@no.abb.com

Abstract

In this paper we present reasons why ZigBee is not considered suitable for use in most industrial applications, which was also motivation for the development of a new wireless communication standard tailored to the industrial needs: WirelessHART. We also give a short presentation of the design features that makes WirelessHART more suitable for industrial applications and requirements.

1 Introduction

HART is a digital protocol for two-way communication between a host application and smart field instruments, providing access to diagnostics, configuration and process data [1]. Traditionally, HART specified a physical layer which used frequency-shift keying (FSK) superimposed on the analog control signal (4-20 mA). As of version 7, HART also incorporates an IEEE 802.15.4-based wireless mesh network as an option for the physical layer. This is commonly referred to as WirelessHART.

In this paper we summarize ABB's impression of the WirelessHART part of the HART7 standard through ABB's participation as a working group member in the standardization committee. ABB also has extensive experience with ZigBee in the past, and we show that the flaws that were identified in ZigBee from an industrial viewpoint, have been addressed in WirelessHART.

1.1 Industrial requirements

ABB has a long history of developing wireless solutions for industry applications. For factory automation ABB developed the frequency hopping Wireless Interface to Sensors and Actuators (WISA) radio technology that was released already in 2001. For process automation ABB has taken a different, more lengthy, approach, actively taking part in various standardization efforts. In 2004 and 2005 ZigBee was the buzz of the industry but testing in industrial environments by ABB revealed it had some deficiencies [2]. The industry demanded secure and reliable communication, but static and multi-path fading sometimes blocked ZigBee due to its use of one static channel.

1.2 Application

The primary use cases for WirelessHART are: 1) access to diagnostics data available in HART-enabled instruments, which are installed in legacy systems that do not speak HART. 2) condition and performance monitoring of critical equipment, which is not part of the control loop due to excessive wiring cost.

1.3 Why use standards?

Key concerns within the automation industry has been the lack of suitable standards to fulfill the above mentioned demands, and also interoperability between different vendors. ABB with its vast experience of wireless in industry applications has shared its knowledge in standardization bodies like ISA100 (Instruments, Systems, and Automation Society) and HCF (HART Communication Foundation) in order to achieve just that.

2 Wireless Standards

2.1 WirelessHART

WirelessHART is designed based on a set of fundamental requirements: it must be simple (e.g., easy to use and deploy), self-organizing and self-healing, flexible (e.g., support different applications), scalable (i.e., fit both small and large plants), reliable, secure, and support existing HART technology (e.g., HART commands, configuration tools, etc).

Figure 1 shows that the architecture of WirelessHART is based on the OSI layer design. WirelessHART is based on the PHY layer specified in the *IEEE 802.15.4-2006* standard [3] [1], but specifies new Data-link (including MAC), Network, Transport, and Application layers.

[1] WirelessHART only supports the 2.4GHz spectrum

978-1-4244-2350-7/08/$25.00 ©2008 IEEE.

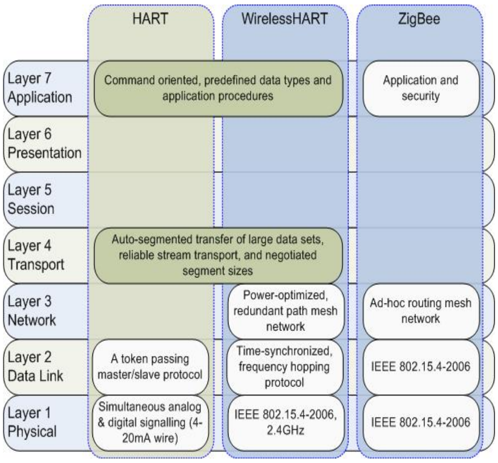
HART
WirelessHART
ZigBee
Layer 7 Application
Layer 6 Presentation
Layer 5 Session
Layer 4 Transport
Layer 3 Network
Layer 2 Data Link
Layer 1 Physical
Command oriented, predefined data types and application procedures
Application and security
Auto-segmented transfer of large data sets, reliable stream transport, and negotiated segment sizes
Power-optimized, redundant path mesh network
Ad-hoc routing mesh network
A token passing master/slave protocol
Time-synchronized, frequency hopping protocol
IEEE 802.15.4-2006
Simultaneous analog & digital signalling (4-20mA wire)
IEEE 802.15.4-2006, 2.4GHz
IEEE 802.15.4-2006

Figure 1. HART, WirelessHART, and ZigBee protocol stacks

Observe that it can also be seen that WirelessHART and HART are compatible at the Transport and Application layers.

2.1.1 Basic features

WirelessHART is a Time Division Multiple Access *(TDMA)* based network. All devices are time synchronized and communicates in pre-scheduled fixed length time-slots. TDMA minimizes collisions and reduces the power consumption of the devices.

WirelessHART uses several mechanisms in order to successfully coexist in the shared 2.4GHz ISM band: *Frequency Hopping Spread Spectrum* (FHSS) allows WirelessHART to hop across the 16 channels defined in the IEEE802.15.4 standard in order to avoid interference. *Clear Channel Assessment* (CCA) is an optional feature that can be performed before transmitting a message, the transmit power level is configurable, and a mechanism to disallow the use of certain channels, called *Blacklisting*, is available. All of these features also ensures WirelessHART does not interfere with other co-existing wireless systems that have real-time constraints.

All WirelessHART devices must have routing capability, i.e., there are no reduced function devices like in ZigBee. Since all devices can be treated equally in terms of networking capability, installation, formation, and expansion of a WirelessHART network becomes simple as the network is self-organizing.

WirelessHART forms mesh topology networks (star networks are also possible, but not recommended), providing redundant paths which allows messages to be routed around physical obstacles, broken links, and interference. Two different mechanisms are provided for message routing: *Graph routing* and *Source routing*. Graph routing uses pre-determined paths to route a message from a source to a destination device. To utilize path redundancy, a graph route consists of several different paths between the source and destination devices. This is the preferred way of routing messages both up- and downstream in a WirelessHART network. *Source routing* uses ad-hoc created routes for the messages without providing any path diversity. Source routing is therefore only intended for network diagnostics, not process related messages.

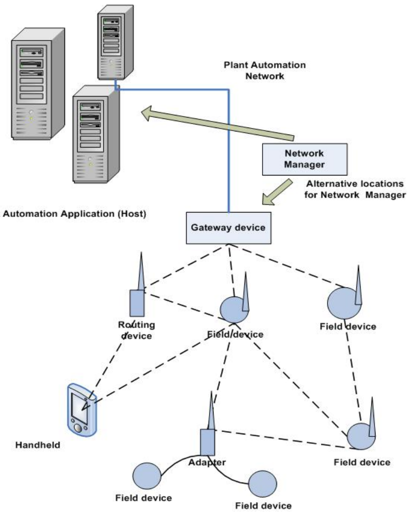

Figure 2. WirelessHART devices and connection to host system.

Figure 2 shows the different Network device types that comprise a WirelessHART network:

Most devices in a WirelessHART network are *Field devices*, which are characterized by being connected to the process, e.g., sensors and actuators.

Router devices are not connected to the process, i.e., lacks the sensor or actuator, instead only having communication functionality. Router devices are not required by the standard, but will be useful in cases where wireless connectivity needs to be improved.

Adapter devices connects wired HART devices to the WirelessHART network, e.g., legacy HART or non-wireless devices. One adapter device can provide wireless network access for more than one wired device as shown in Figure 2.

Handheld devices are used for the installation, configuration, monitoring, and maintenance of all kinds of WirelessHART devices. A Handheld device can either be: 1) connected to the plant automation network through another wireless network (e.g. WLAN, Bluetooth, etc) and talking to the WirelessHART devices through the plant automation host, 2) connected directly to the WirelessHART network as a WirelessHART device as shown in Figure 2.

The *Gateway device* connects the WirelessHART network to the plant automation system (host). It provides the host system with access to WirelessHART Network devices and will, if required, translate between different protocols.

The *Network Manager* is the centralized "brain" of the

WirelessHART network.Its responsibility is to manage everything related to the wireless network, e.g. forming the network, scheduling resources, network path configuration and reconfiguration, etc. Only one active Network manager can exist per WirelessHART network, with the possibility to have a backup manager to take over if the active one fails.

2.1.2 Security

Security is mandatory in WirelessHART; there is no option to turn it completely off. WirelessHART provides end-to-end and hop-to-hop security measures through payload encryption and message authentication on the Network and Data-link layers. However, the security measures are transparent to the Application layer. WirelessHART uses CCM* [2] mode in conjunction with AES-128 block cipher using symmetric keys, for the message authentication and encryption.

A set of different security keys are used to ensure secure communication: A new device is provisioned with a *Join key* before it attempts to join the wireless network. The Join key is used to authenticate the device for a specific WirelessHART network. Once the device has successfully joined the network, the Network manager will provide it with proper Session and Network keys for further communication. The actual key generation and management is handled by a "plant wide" *Security manager*, which is not specified by WirelessHART, but the keys are distributed to the Network devices by the Network manager. A *Session key* is used by the Network layer to authenticate the end-to-end communication between two devices (e.g., a Field device and the Gateway). Different Session keys are used for each pairwise communication (e.g., Field device to Gateway, Field device to Network manager, etc). The Data Link layer uses a *Network key* to authenticate messages on a one-hop basis. A well known Network key is used when a device attempts to join the network, i.e., it before it has received a proper Network key.

Keys are rotated based on the security procedures of the process automation plant.

2.2 ZigBee

ZigBee is a specification for a cost-effective, low-rate and low-power wireless communication protocol for home automation, monitoring and control. It aims to provide short range wireless networking which is scalable, self-organizing and secure, while providing battery life up to two years. Although having existed since late 2004, ZigBee has yet to prove its success, at least in the industrial domain where reliability and security are uttermost important. In this section we give a short technical introduction to ZigBee, providing the background for our comparison to *WirelessHART* in the next section.

2.2.1 Basic features

ZigBee is a specification for the higher protocol layer, and builds upon the physical (PHY) and medium-access control (MAC) layers in the 802.15.4 specification [3], Figure 1. Mesh networking topology is supported and routing is achieved through the ad-hoc on-demand distance vector (AODV) algorithm. This means that it is the devices themselves that are responsible for route discovery, and peer-to-peer communication is possible. In a ZigBee network, all nodes shares the same channel, and frequency agility is minimal. There is no frequency hopping, and the only option is to scan for a channel with the least amount of interference at startup. There are two classes of network devices in ZigBee; Full-Function Devices (FFD) and Reduced-Function Devices (RFD). The former can route messages in mesh networks and act as the network coordinator, whereas the latter can only communicate with one FFD in a star network setup.

ZigBee can operate in both beaconed and non-beaconed mode. In the beaconed mode, the nodes are to some extent synchronized and the superframe is divided into 16 slots. The slots in the frame are generally contention-based, using CSMA/CA[3]. There is an option to use up to seven of these as dedicated slots to specific nodes to increase determinism, so-called guaranteed slot time (GTS). However, support for this is not mandatory and use of this feature might break interoperability.

2.2.2 Security

In the 2006 version of the specification, security is not mandatory. However, support for authentication, integrity and encryption for both network and application layer is present. MAC layer security available through 802.15.4 is not explicitly addressed in the ZigBee standard, and its use might break interoperability between different vendor's products. Replay attacks is protected against using sequential numbering. ZigBee makes use of the security mechanisms in 802.15.4; Counter with CBC-MAC[4] (CCM) with AES-128 encryption, but with the option to employ encryption-only or integrity-only. Three key types are used: *Master key*, *Link key* and *Network key*. The master key is comparable to the join key in WirelessHART and is necessary to join the network. The link key is used for end-to-end encryption and would by that provide the highest level of security at the price of higher storage requirements. The network key is shared between all devices, and thus presents a lower level of security, though with the benefit of reduced storage requirements in the devices. All keys can be set at the factory, or be handed out from the trust center (residing in the network coordinator), either over the air, or through a physical interface.. For commercial grade application, the trust center can control the joining of new devices and periodically refresh the network key.

[2] Counter with CBC-MAC, with option to have encryption-only or authentication-only modes

[3] Carrier-Sense Multiple Access with Collision Avoidance

[4] Cipher Block Chaining - Message Authentication Code

3 Comparison

Although ZigBee has had very limited success in the marketplace so far, comparing it with WirelessHART is interesting since the former is well known in both academia and the industry. By discussing the weaknesses that ZigBee have been criticized for from the industry, we can analyze WirelessHART's probability of success by looking at how it addresses the criticism of ZigBee.

3.1 ZigBee

Since any problems with the equipment translates to economical loss for an industrial user, reliability is a primary concern for these users. Hence, parameters like network robustness, reliable message delivery, authentication and integrity are all important for industrial use. Moreover, the threat of industrial espionage advance the requirement for encryption to hide information that can reveal anything about the production in the plant to competitors.

One of the loudest argument against ZigBee has been the lack of industrial-grade robustness. First of all, there is no frequency diversity since the entire network shares the same static channel, making it highly susceptible to both unintended and intended jamming. This also means that the severe frequency selective fading due to the metal-rich propagation environments in plants potentially can stop all ZigBee communication. Moreover, the static channel will also increase interference for other systems like wireless-LAN, and increase delay as the network size grows and collisions forces retransmissions. Secondly, there is no path diversity meaning that in case of a link is broken, a new path from source to destination must be set up. This increases both delay and overhead, and route-discovery will eventually consume all bandwidth available in environments with unstable routes. Furthermore, the lack of robustness also means that ZigBee is less suited for control applications.

Battery operation for routers with many peers is not realistic, since the CSMA/CA forces it to keep its receiver on for a large part of the frame.

Security in ZigBee can to a great extent be set up to meet the requirements from industrial users, although care must be taken to use equipment from vendors which support the necessary security mechanisms.

3.2 WirelessHART

WirelessHART addresses some of the main concerns raised by the industry towards ZigBee. It's designed from start to be a robust and secure communications protocol; thus implementing many features in order to achieve it. Frequency hopping and retransmissions limits the effects of temporal and frequency interference (a retransmission will occur on a different frequency). This also limits the interference WirelessHART causes on other networks. Mesh networking with graph routing provides path redundancy and self-healing properties that limits the effect of broken links. The robustness of WirelessHART opens up the possibility for wireless control, at least for slow and non-critical processes. The use of TDMA and pre-scheduled timeslots prevents message collisions and allows devices to increase their power savings because the device only needs to keep the radio on during the required timeslots. The cost of TDMA is that time-synchronization is required; but, in WirelessHART the time information requires no additional network traffic because it is embedded in the automation process related traffic.

WirelessHART is a secure protocol and provides several layers of protection. All traffic is secured; the payload is encrypted and all messages are authenticated, both on a single-hop basis as well as end-to-end. WirelessHART requires that all devices are provisioned with a secret Join key as well as a Network id in order to join the network.

4 Summary

In this paper we present WirelessHART, a recently released industrial wireless network standard, and compare it to ZigBee in areas that are interesting for industrial applications. The comparison shows that WirelessHART addresses many of the weaknesses that ZigBee has been criticized for, and thus has the potential for success in industrial applications.

	ZigBee	WirelessHART
Robustness	Low	High
Co-existence	Low	High
Power consumption	High	Low
Security	Low	High

Table 1. Overview of comparison

The WirelessHART standard specifies the communication stack, as well as the interfaces and responsibilities for the various devices comprising a WirelessHART network. However, it does not specify how these responsibilities should be accomplished, which provides many opportunities to create improved and optimized solutions. The Network Manager is an example of such a device, its responsibility is to manage all aspects related to the wireless network, but how it should do this is an open question.

References

[1] HCF - HART Communication Foundation, "HART7 Specification", September 2007.

[2] N. Aakvaag, M. Mathiesen, and G. Thonet, "Timing and Power Issues in Wireless Sensor Networks - an Industrial Test Case", in *Proceedings of the 2005 International Conference on Parallel Processing Workshops*, June 2005, Oslo, Norway.

[3] I. C. Society, "Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs)", Technical report, IEEE Computer Society, 2006.