Contents

WirelessHART 1
Motivation 1
Introduction 1
Components of WirelessHART 2
The WirelessHART Protocol 3
The WirelessHART Physical Layer 4
Interfaces 5
Conclusion 5
References 6

WirelessHART

Motivation

Traditionally, industrial process and automation networks have been wired networks, implying increased deployment and maintenance costs. Many efforts have been made to introduce wireless technology into the process sector as the development of Wireless Sensor Networks (WSN) has progressed. The major arguments for selecting a wireless solution in industrial applications are the lower cost and easier installation and deployment of wireless components.
WirelessHART (Wireless Highway Addressable Remote Transducer) is the first open wireless communication standard specifically designed for process measurement and control applications[1]. WirelessHART complements the ever so successful HART field devices by providing the possible means for communicating via wireless channels[2].

Introduction

In the field of industrial control, wireless process control has recently been a popular topic. WirelessHART is an emerging communication protocol for industrial automation. It is an extension of the widely used Highway Addressable Remote Transducer (HART) communication protocol. On March 2010 WirelessHART was approved by the International Electrotechnical Commission (IEC) as a first international standard for industry process automation[3]. Furthermore, On June 2010 it was approved as the First European National Standard for Wireless Communication in Process Automation by the European Committee for Electrotechnical Standardization (CENELEC). WirelessHART promises to bring the heritage of simplicity and robustness the customers know from the earlier revision of the HART standard. Before WirelessHART ZigBee and Bluetooth can't meet the stringent requirements of industrial control. Neither ZigBee nor Bluetooth makes any effort to provide a guarantee on end-to-end wireless communication delay. The new WirelessHART is specifically targeted to those problems in ZigBee & Bluetooth and provide solution for process control applications.

WirelessHART uses the 2.4GHz ISM radio frequency, which is unrestricted. It uses IEEE 802.15.4 low-rate wireless personal area networks (LR-WPANs) as the physical layer at the very bottom. WirelessHART defines its own time-synchronized MAC layer on top of that. WirelessHART MAC includes industry-standard AES-128 ciphers and keys, as well as a rigorous 10ms time slot, network-wide time synchronization, channel blacklisting, and channel hopping. Reliability is achieved using methods of frequency diversity, path diversity and message delivery retrials. Power Consumption can be efficiently optimized by a proper management of the communications schedule. Self-organizing and self-healing mesh networking approaches are supported by the network layer. Messages can be routed around interferences and impediments in this fashion. WirelessHART further stands out from other open protocols by employing a central network management. The network manager is in charge of keeping the network's routes and communication schedules up to date, ensuring network performance.

	Bluetooth	**ZigBee**	**WirelessHART**
Security	Optional	High	Very High
Reliability	Low	Very Low	High
Power Consumption	High	Medium	Low
Scalability	Limited	Medium	High

Table 1. Comparative table of Bluetooth, ZigBee and WirelessHART

Components of WirelessHART

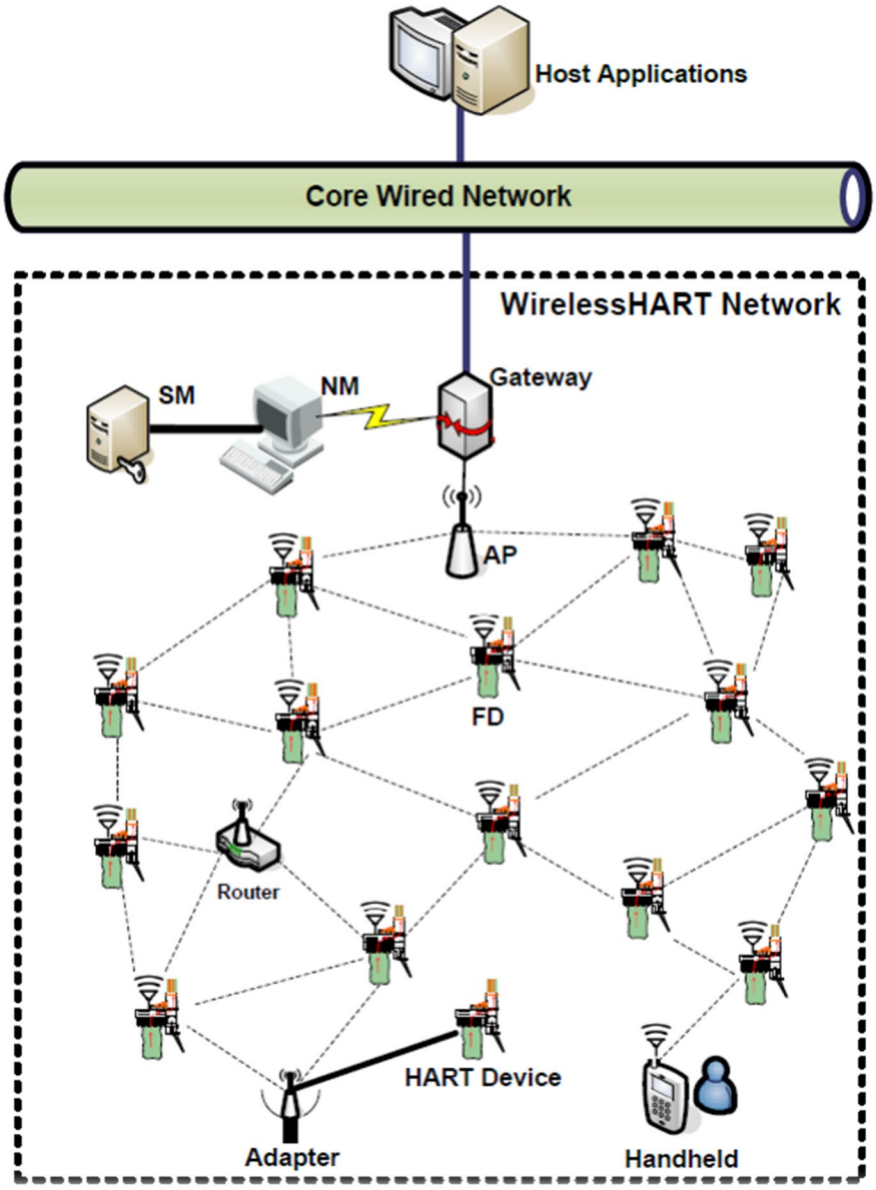

Figure 1. WirelessHART Network Components[4]

Figure 1 shows the generic WirelessHART mesh network which contain the following components:

Network Manager (NM) : It is the application responsible for forming and configuring the network, scheduling communication between devices, managing the routing in the network and monitoring and reporting the health of the network. There is only one active Network Manager per WirelessHART network.

Security Manager (SM): Application responsible of managing the security resources, that is the security keys, and monitoring the status of the network security.

Gateway (GW): Divided into virtual Gateway and the Access Points (AP) (1 or more). It is the link between the host applications, Network manager and the wireless HART network. Responsible of buffering, protocol conversions and clock source.

Field Devices (FD) The actual sensors distributed in the industry process capable of routing and forwarding packets.

Host applications: User applications connected to the backbone network of the industry that communicate with Field Devices on behalf of fetching process and control data. The Gateway is the connection point between host applications and the WirelessHART Network.

Adapters: They are the devices providing backwards compatibility by adding wireless HART capabilities to wired HART devices. It can provide wireless access to one or more devices.

Handheld Host application residing on a portable device. Its aim is the configuration, monitoring, calibrating and maintenance of devices. It can be connected to the WHART network or the plant automation network.

Routers Devices: It is capable of routing and forwarding packets in the network. However, they are not connected to the industrial process (sensors or actuators). They are required when wireless connectivity needs to be improved.

The WirelessHART Protocol

WirelessHART has a number of basic capabilities and even greater amount of additional features that can be configured. Figure 1 illustrates the architecture of the WirelessHART protocol stack according to the OSI 7-layer communication model. As shown in this figure. 2, WirelessHART protocol stack includes five layers:

- Physical Layer
- Data-Link Layer
- Network Layer
- Transport Layer
- Application Layer

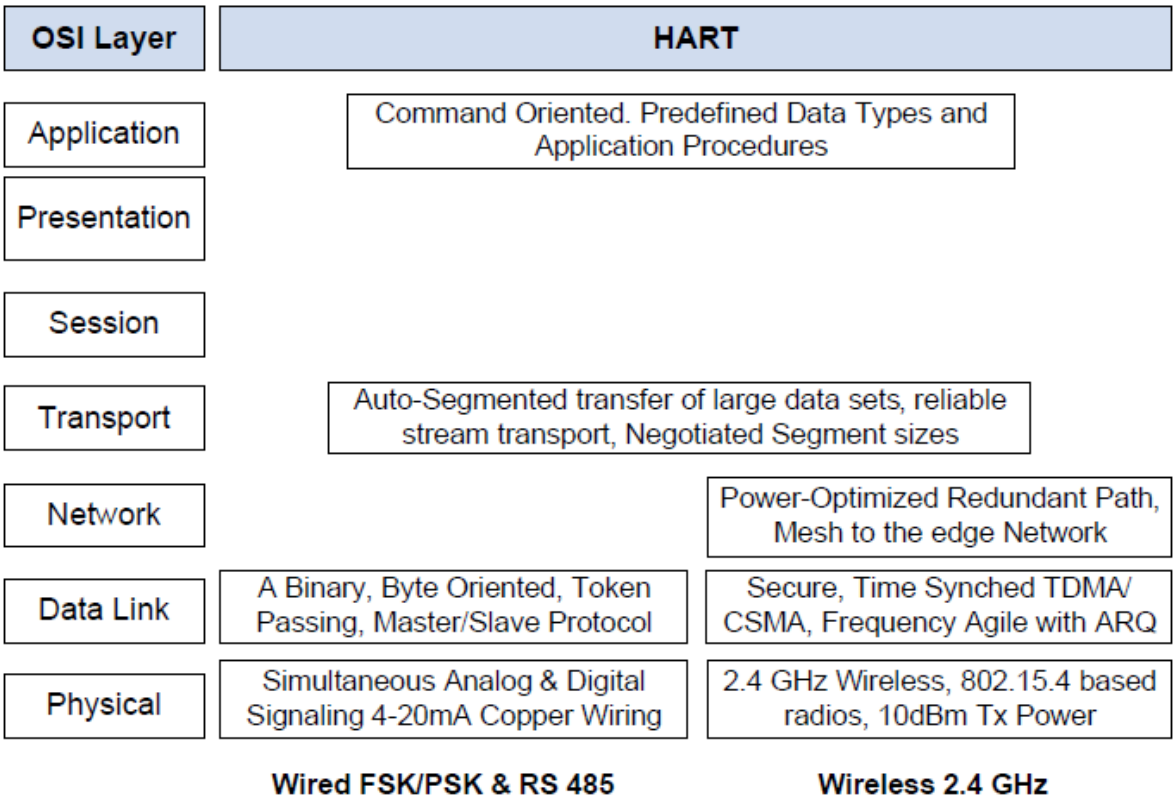

Figure 2. Architecture of HART Communication Protocol [1]

Reliable data transmission is ensured through a combination of PHY layer, MAC, network and transport layer mechanisms. That is, FHSS, DSSS to combat the fading and interference in the wireless channel, link level ACK to trigger retransmission when needed, path diversity in graphic routing and transport protocol with end-to-end acknowledgements.

The WirelessHART Physical Layer

Physical layer is responsible for signaling, modulation and actual transmission of data. The WirelessHART protocol employs the partially adopted [5] IEEE 802.15.4- 2006. It employs O-QPSK (Offset Quadrature Phase Shift Keying) and operating at 2.4GHz unlicensed band with data rate up to 250 kbps. Its channels are numbered from 11 to 26, with a 5MHz gap between two adjacent channels. DSSS is utilized to resist interference from jamming. It is combined with FHSS, where the radio carrier hops over multiple frequency bands(channels) using a pseudo random sequence. FHSS is effective in overcome narrow band interference such as that from multipath fading. The Physical Layer PDU (PPDU) (figure 3) begins with a synchronization header (SHR). The SHR consists of a preamble sequence followed by a Start of Frame Delimiter (SFD).

Figure 3. WirelessHART Physical PDU Structure [6]

The SHR is always transmitted first for any WirelessHART frame. For the 2.4 Ghz Physical Layer the preamble sequence length is 4 bytes and the SFD length is 1 byte. The preamble field is used by the transceiver to obtain chip and symbol synchronization with an incoming message. The SFD field indicates an end of the SHR and a start of a packet data. A length field is 7 bits in length, it specifies the total number of bytes contained in the PPDU payload excluding itself.
The PHY data service enables the transmission and reception of PHY protocol data units (PPDUs) across the physical radio channel.

The “hidden terminal”-like problem in TDMA schedule can be avoided by requiring each link operating on a different frequency, which is easily applicable in WirelessHART the PHY layer utilizes frequency hopping.

Currently the PHY layer of the network devices complies to the IEEE 802.15.4 standard, which is designed for low power, low data rate devices with low complexity.

Interfaces

The interface between the PHY and Datalink layer describes the service primitives provided by the physical layer, and the interface between the Datalink and NETWORK layer defines the service primitives provided to the network layer.

Conclusion

WirelessHART employs the 2.4GHz license-free frequency band, which was created with industrial wireless sensor communications in mind. TDMA, which synchronizes the devices that make up the network in 10 ms stages, is used to coordinate communication. This allows for a highly dependable (collision-free) network while also lowering the amount of time a station must be active [[7]. WirelessHART can coexist with different wireless networks because it is based on the IEEE 802.4.15 standard. It's a self-healing network that checks for damage, fixes itself, and discovers alternate routes around obstacles [8]. It also offers strong security features like AES-128 encryption, code management, and authentication to keep data and the network safe.

References

[1] J. Song *et al.*, “WirelessHART: Applying Wireless Technology in Real-Time Industrial Process Control,” in *2008 IEEE Real-Time and Embedded Technology and Applications Symposium*, St. Louis, MO, USA, Apr. 2008, pp. 377–386. doi: 10.1109/RTAS.2008.15.

[2] A. N. Kim, F. Hekland, S. Petersen, and P. Doyle, “When HART goes wireless: Understanding and implementing the WirelessHART standard,” in *2008 IEEE International Conference on Emerging Technologies and Factory Automation*, Hamburg, Germany, Sep. 2008, pp. 899–907. doi: 10.1109/ETFA.2008.4638503.

[3] “Homepage | FieldComm.” https://www.fieldcommgroup.org/ (accessed June 05, 2022).

[4] J. H. Sánchez, “Software Design and Architecture,” p. 93.

[5] “HART Protocol Specifications | FieldComm.” https://www.fieldcommgroup.org/hart-specifications#230548828-3027987918 (accessed June 05, 2022).

[6] I. Konovalov, “A Framework for WirelessHART Simulations,” p. 49.

[7] “WirelessHART - Wireless Technology | HART interface solutions.” https://www.pepperl-fuchs.com/global/es/10028.htm (accessed June 05, 2022).

[8] by, “Wireless HART Communication Protocol Overview,” *Inst Tools*, Jun. 19, 2016. https://instrumentationtools.com/wireless-hart-communication-protocol-overview/ (accessed June 05, 2022).