Design and Simulate the Communication of Instrument and Control Systems using WirelessHART

Nguyen Huy Phuong, Cao Ngoc Khanh, Bui Dang Thanh*

Hanoi University of Science and Technology - No.1, Dai Co Viet, Hai Ba Trung, Hanoi, Viet Nam

Received: November 06, 2018; Accepted: November 28, 2019

Abstract

The WirelessHART protocol is one of the most promising standards for wireless communication in industrial automation plant systems. Control processes as well as the communication between plants in the systems need to be scheduled appropriately such that the input and output data is correlated. This paper presents a design and simulation of the communication of instrument and control system using wirelessHART. In addition, the paper presents design methods, options for instrument and control systems. Moreover, in this study, we also develop network simulation program to evaluate the communication of instrument and control systems. A number of improvements have been made and then compared with previou works in terms of energy consumption, ensuring the stability of communication.

Keywords: WirelessHART, IEEE 802.15.4, IEC 62591, Network design, Communication simulation, NS-2

1. Introduction

WirelessHART is an interoperable wireless standard for process measurements and control applications [1, 2]. Compare to other wireless standards such as ZigBee and Bluetooth standards, WirelessHART has some advantages such as it meets the stringent requirements of industrial control. It is scalable enough for using in large scale process control systems. There are many studies to develop and apply the WirelessHART in the literatures. De Deminicis et al. [3] developed a WirelessHART simulator (for the PHY and MAC layers) to explore coexistence problems. De Biasi et al. [4] developed a WirelessHART simulator to investigate the clock drift in process control. Nixon et al. [5] presented an approach used a wireless mesh network to meet control performance requirements. Meanwhile, several approaches have been taken towards simulating wireless sensor networks [5, 6].

In this study, we design instrument control systems using WirelessHART. The design is applied for the case: the system including 51 nodes (1 Gateway and 50 nodes), 100m x 100m flat coordinate system. The distance between nodes is about 7m. The system consists of 15 pairs of sensor-actuator. Scenario of communication simulation for instrument control system using WirelessHART is 120,000 seconds.

2. Architecture of WirelessHART network

The WirelessHART protocol has been designed in order to implement a sensor and actuator mesh communication system. A typical topology of a WirelessHART network [2, 6] showing its architecture is depicted in Fig. 1. Devices in a network are presented as in following:

- *Network Manager* per network, which forms the network, handles node affiliation, schedules resources configure routing paths, monitors and reports the network health, etc.

- *Security Manager* uses to handle security issues, e.g., the distribution of encryption keys to the network manager in each network.

- *Routers* are deployed in the network to improve network coverage and connectivity. In WirelessHART, the routing role is executed by field devices.

- *Access Points* are attached to the gateway and provide redundant paths between the wireless network and the gateway.

- *Gateway*, whose task is to interconnect field devices with the plant automation system by exploiting one or more access points.

- Several *field devices*, i.e., sensors and actuators, connected to the process. These devices are able to participate in routing tasks.

* Corresponding author: Tel.: (+84) 915.897.699
Email: thanh.buidang@hust.edu.vn

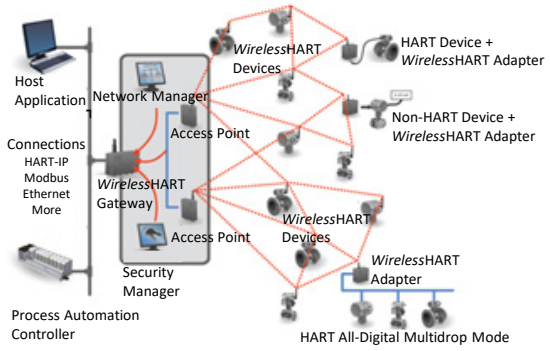

Fig. 1. Typical topology of WirelessHART network

2.1 Communication in WirelessHART network

The WirelessHART physical layer is based mostly on the IEEE 802.15.4-2006 2.4GHz DSSS physical layer [7]. This layer defines radio characteristics, such as the signaling method, signal strength, and device sensitivity. The WirelessHART protocol operates in the 2400-2483.5MHz license-free ISM band with a data rate of up to 250 kbps. Its channels are numbered from 11 to 26, with a 5MHz gap between two adjacent channels.

The data link layer provides the reliable means to transfer data between network nodes by detecting and possibly correcting errors that may occur in the physical layer. This layer has the important task of creating and managing data frames. The data link layer introduces the use of super frames and time dimension multiple access (TDMA) technology to provide collision free, deterministic communication. Timeslots 10ms in length are grouped into super frames. These super frames are used to control the timing of transmissions to insure reliable communication and reduce collisions.

The data link layer employs channel hopping and channel blacklisting to increase security and reliability. In channel hopping, every time a transmission occurs, the channel is switched. Channel blacklisting identifies channels consistently affected by interference and removes them from use. There are usually two sublayers:

- *Logical Link Control* (LLC) requirements including the format of HART frames, the structure of HART device addresses; the security services used for message integrity and the error detection coding to be used.

- *Media Access Control* (MAC) rules ensuring that transmissions by devices occur in an orderly fashion.

The network and transport layers cooperate to handle various types of traffic, routing, session creation, and security. WirelessHART establishes a mesh network, requiring each device be able to forward packets for other devices. In reality, the network layer functions as a combined network/transport/session layer, handling all the function required by the protocol in those three layers of the OSI model. WirelessHART presents two main approaches for routing packets: graph routing and source routing

- *Graph routing*: A graph is a collection of paths that connect network nodes. The paths in each graph is explicitly created by the network manager and downloaded to each individual network device. To send a packet, the source device writes a specific graph ID (determined by the destination) in the network header.

- *Source routing* is a supplement of the graph routing aiming at network diagnostics. To send a packet to its destination, the source device includes in the header an ordered list of devices through which the packet must travel. As the packet is routed, each routing device utilizes the next network device address in the list to determine the next hop until the destination device is reached.

2.2 Security in WirelessHART network

A WirelessHART network is a secure network system. Both the MAC layer and network layer provide security services [1, 2]. The MAC layer provides hop-to-hop data integrity by using a combination of a cyclic redundancy check (CRC) and a Message Integrity Code (MIC). Although the CRC has limited value it is still used. Both the sender and receiver use the CCM* mode together with AES-128 as the underlying block cipher to generate and compare the MIC.

The network layer employs various keys to provide confidentiality and data integrity for end-to-end connections. Four types of keys are defined in the security architecture:

- *Public key* is used to generate MICs on the MAC layer when network key is not applicable.

- *Network keys* which are shared by all network devices and used by existing devices in the network to generate MAC MIC's.

- *Join keys* that are unique to each network device and is used during the joining process to authenticate the joining device with the network manager.

- *Session keys* that are generated by the network manager and are unique for each end-to-end connection between two network devices. They provide end-to-end confidentiality and data integrity.

3. Design instrument control systems using WirelessHART

The International Society of Automation (ISA) considers six classes of applications, from critical control to monitoring, in which the importance of the message timeliness and quality of service (QoS) requirements decreases from Class 0 to 5 in Table 1. WirelessHART supports industrial applications ranging from Class 2 to 5.

According to the above classification, if a fully functional ICSS system installed in the plant includes the Process Control System (PCS), Safety Instrumented System (SIS) and Fire and Gas System (FGS), WirelessHART can only use partly in PCS system. While WirelessHART performs well in monitoring and on/off controls. WirelessHART should not be used temporarily in closed loop controls such as PID control for control valves until the notable improvement (Tables 2 and 3).

Table 1. Application of wireless protocols evaluation

Category	Class	Application	Description
Safety	0	Emergency action	Always critical
Control	1	Closed-loop regulatory control	Often critical
	2	Closed-loop supervisory control	Usually noncritical
	3	Open-loop control	Human in loop
Monitoring	4	Alerting	Short-term operational consequence
	5	Logging and downloading/uploading	No immediate operational consequence

Table 2. Selecting right protocol

	Safety System	Critical Control	On-Off Control	In-plant Monitoring	Remote Monitoring
Wired HART					
Fieldbus					
WirelessHART					

Table 3. Selecting right signal type

	Analog Input	Analog Output	Digital Input	Digital Output
Wired HART				
Fieldbus				
WirelessHART				

Legend	Based on technical/commercial consideration
	Most appropriate solution
	Appropriate in some cases
	Lease effective solution

Follow these three key steps bellow for designing a network [8, 9]:

a. *Scope* – Decide if we need to reference wireless field networks by process unit or subsection of a process unit. Factors include:

- Number of devices in the process unit
- Update rates need for wireless devices
- Capacity of the Gateway

Use the following calculation to determine the number of Gateways:

$$\#\text{gateway} = \text{ROUNDUP}\left(\frac{\text{Total WirelessHART devices in process unit}}{\text{Gateway capacity} * (1 - \text{spare requirement})}\right)$$

In the last section, we will perform a network simulation of 50 nodes, using Gateway 1420 able be used with up to 100 devices, storage capacity is 25%, so the number of Gateway needed is:

$$\#\text{gateway} = \text{ROUNDUP}\left(\frac{50}{100*(1-0.25)}\right) = 1$$

In addition, the Gateway can be deployed for network redundancy if the measurements are important.

The effective range of a device is the typical linear distance between WirelessHART field devices when in the presence of process infrastructure. Below there are three basic classifications for effective range in the process environment.

- Heavy obstruction – 30 m. This is the typical heavy density plant environment; where a truck or equipment cannot be driven through.

- Medium obstruction – 75 m. This is the less light process areas where a lot of space exists between equipment and infrastructure.

- Light obstruction – 150 m. Typical of tank farms. Despite tanks being big obstructions themselves, lots of spaces between and above makes for good RF propagation.

- Clear line of sight – 230 m. The antenna for the device is mounted above obstructions and the angle of the terrain change is less than five degrees.

Some WirelessHART vendors provide options and techniques for obtaining even further distances for long distance applications.

b. *Design* – Apply design rules to ensure optimum connectivity. There are four fundamental, recommended network design rules:

- *"Rule of Five Minimum"*-Every WirelessHART network should have a minimum of five WirelessHART devices within effective range of the Gateway.

- *"Rule of Three"* – Every WirelessHART device should have a minimum of three neighbors with in effective range.

- *"Rule of Percentages"* – Every WirelessHART network with greater than five devices should have a

minimum of 25 percent of devices within effective range of the Gateway to ensure proper bandwidth and eliminate pinch points.

- *"Rule of Maximum Distance"* – Wireless devices with update rates faster than two seconds should be within two times the effective range of wireless devices from the Gateway.

c. *Fortify* – Identify and correct any potential weaknesses in the network design. It is recommended to stress test the network design by altering the effective range of devices in order to identify potential weaknesses in the network design.

4. Simulation of communication

WirelessHART simulation is implemented on NS-2 software [9]. Because NS-2 runs on the Lunix operating system, to install NS-2 on the Windows operating system, we first install Ubuntu 16.04 LTS on a VMWare virtual machine. Then, install *ns-2.35* on Ubuntu. The *ns-2.35* software is the final version of NS-2, which supports IEEE 802.15.4 but does not support WirelessHART. Based on the library available, Pouria Zand has edited to create a library of layers for WirelessHART. Finally, integrate the WirelessHART library into the *ns-2.35* software as shown in Fig. 2.

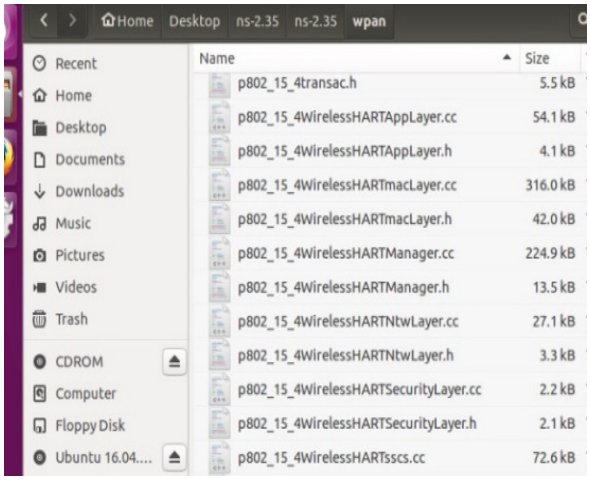

Fig. 2. WirelessHART library files in ns-2.35

Scenario of communication simulation for instrument control system using WirelessHART:

- 51 nodes including 1 Gateway and 50 nodes.
- 100 m x 100 m flat coordinate system.
- Distance between nodes ~ 7m (Fig. 3).
- Simulation time is 120,000 seconds.
- 15 pairs of sensor- actuator as listed in Table 4.

Table 4. List of sensor-actuator pairs

No.	Sensor	Actuator	8	18	24
1	3	5	9	22	19
2	6	7	10	20	23
3	15	8	11	27	36
4	9	14	12	46	49
5	10	13	13	28	35
6	26	16	14	29	34
7	17	25	15	33	30

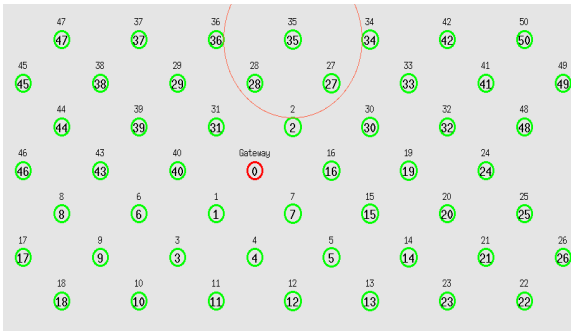

Fig. 3. Nam animation program

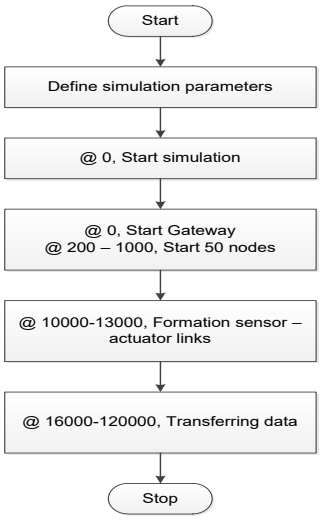

Fig. 4. Flowchart of simulation scenario

The result is a program that illustrates nodes including initialization, data transferring, and trace files that record all the parameters during the simulation. The nodes that are launched will change the status color. Transferring data will appear as circles.

Scenario simulation as listed as flowchart in Fig. 4:

- At 0 seconds, Gateway starts up
- From 200 seconds to 1000 seconds, the 1-50 nodes start

- From 10000 to 13000 seconds, the sensor-actuator pairs links form
- From 16000 to 120,000, the process of transferring data
- End of simulation at 120,000 seconds.

In the simulation program, we will apply the *Energy Model*. Here we use the Texas Instrument CC2500 chip parameters.

- Energy initially: 1000 Joules
- Transmission power: TxPower = 37.8 mW
- Receive power: RxPower = 27 mW
- Idle power: IdlePower = 2.7 mW

Sleep power: SleepPower = 1.6 uW

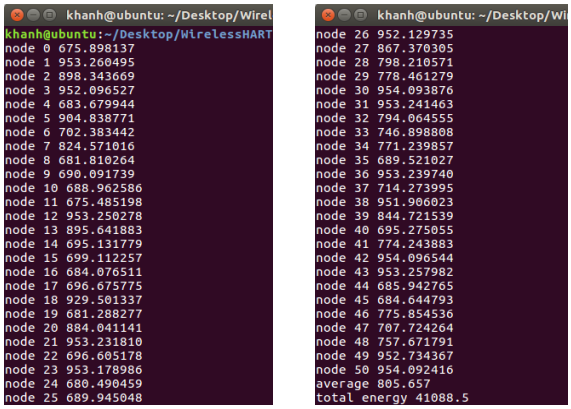

Fig. 5. Residual energy of nodes after simulation

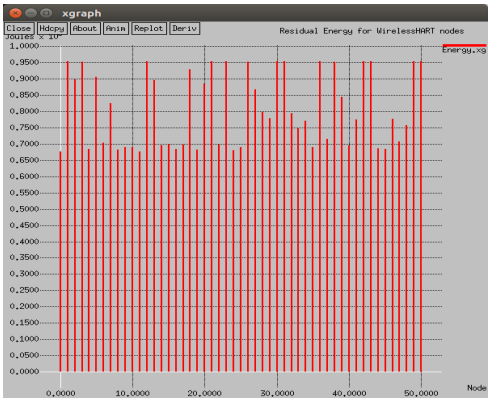

Fig. 6. Residual energy graph by x-graph

Use the additional subprogram *Energy.awk* to extract data from the trace file to compute the residual energy levels of each node after the simulation as presented in Fig. 5.

Graph of the residual energy of nodes using *Xgraph* program is shown in Fig. 6. Besides, we can use a different subprogram *Packet.awk* to calculate the total number of Generated Packets and Received Packets (Fig. 7):

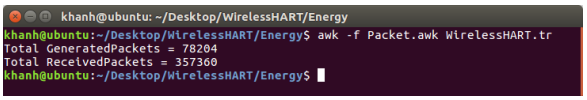

Fig. 7. Total sent and received packet within simulation

5. Conclusion

We have presented designing instrument control systems using WirelessHART. It has been shown that the approach in this paper is feasible to deploy WirelessHART technology in processing plants. The results from the simulation process for the case including 51 nodes, 100 m x 100 m flat coordinate system, distance between nodes, 15 pairs of sensor–actuator have been demonstrated the good performances of the approach.

References

[1] Chen D., Nixon M., Mok A., WirelessHART: Real-Time Mesh Network for Industrial Automation, Springer, 2010.

[2] Emerson Process Management, System Engineering Guidelines IEC 62591 WirelessHART®, USA, 2016.

[3] C. De Dominicis, P. Ferrari, A. Flammini, E. Sisinni, M. Bertocco, G. Giorgi, C. Narduzzi, F. Tramarin, Investigating WirelessHART coexistence issues through a specifically designed simulator, The Intl. Instrumentation and Measurement Technology Conference, 2009.

[4] M. De Biasi, C. Snickars, K. Landernäs, A. Isaksson, Simulation of Process Control with WirelessHART Networks Subject to Clock Drift, The 32nd IEEE Intl. Computer Software and Applications Conference, 2008.

[5] M. Nixon, D. Chen, T. Blevins, A. K. Mok, Meeting control performance over a wireless mesh network, The 4th IEEE Conference on Automation Science and Engineering, 2008.

[6] Han S., Zhu X., Chen D., Mok A.K., Nixon M., Reliable and Real-time Communication in Industrial Wireless Mesh Networks, IEEE Real-Time and Embedded Technology and Applications Symposium, Chicago, USA, pp. 3-12, 2011.

[7] IEEE, 802.15.4-2006 Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs), USA, 2006.

[8] Kim A.N., Hekland F., Petersen S., Doyle P., When HART Goes Wireless: Understanding and Implementing the WirelessHART Standard, IEEE International Conference-Emerging Technologies and Factory Automation, Hamburg, Germany, 2008.

[9] Zand P., Dilo A., Havinga P., Implementation of WirelessHART in NS-2 simulator, IEEE 17th Conference-Emerging Technologies & Factory Automation, Krakow, Poland, 2012.