A Passive Monitoring Tool for Evaluation of Routing in *Wireless*HART Networks

Gustavo Kunzel[1], Jean Michel Winter[1], Ivan Muller[1], Carlos Eduardo Pereira[1], and João Cesar Netto[2]

[1] Federal University of Rio Grande do Sul, Electrical Engineering Dept., Porto Alegre, Brazil
{gustavo.kunzel,jean.winter,ivan.muller}@ufrgs.br,
cepereira@ece.ufrgs.br
[2] Federal University of Rio Grande do Sul, Informatics Dept., Porto Alegre, Brazil
netto@inf.ufrgs.br

Abstract. Wireless communication networks have received strong interest for applications in industrial environments. The use of wireless networks in automation systems introduces stringent requirements regarding real-time communication, reliability and security. The *Wireless*HART protocol aims to meet these requirements. In this protocol, a device known as Network Manager is responsible for the entire network configuration, including route definition and resource allocation for the communications. The route definition is a complex process, due to wireless networks characteristics, limited resources of devices and stringent application requirements. This work presents a tool that enables the evaluation of the topology and routes used in operational *Wireless*HART networks. By capturing packets at the physical layer, information of operating conditions is obtained, where anomalies in network topology and routes can be identified. In the case study, a *Wireless*HART network was deployed in a laboratory, and by the developed tool, important information about the network conditions was obtained, such as topology, routes, neighbors, superframes and links configured among devices.

Keywords: *Wireless*HART, Wireless industrial networks, Routing.

1 Introduction

The deployment of wireless networks in real-world control and monitoring applications can be a labor-intensive task [1]. Environmental effects often trigger bugs or degrade performance in a way that cannot be observed [2]. To track down such problems, it is necessary to inspect the conditions of network after devices deployment. The inspection can be complex when commercial equipment is used in applications. It can be difficult to gather specific information about the performance of the network, according to the limited visibility provided by the equipments.

Wireless networks has stringent requirements on reliable and real-time communication [3, 22] when used in industrial control applications. Missing or delaying the process data may severely degrade the control quality. Factors as signal strength variations, node mobility and power limitation may interfere on overall performance.

G. Schirner et al. (Eds.): IESS 2013, IFIP AICT 403, pp. 159–170, 2013.

Recently, the International Electrotechnical Commission certified the *Wireless*HART (WH) protocol as the first wireless communication standard for process control [4]. The good acceptance of the protocol by the industry has ensured the developing of different devices that meet the standard from several manufacturers. However, it can be seen that there is still a great lack of computational tools that allow a clearer examination of the behavior and characteristics of these networks and devices [5]. Many of these tools become essential as soon as the full operation of the network depends and varies according to the aspects of the environment as well as the distribution of devices.

The WH network enables mesh topologies, where all the devices have the task of forwarding packets to and from other devices. The Network Manager (NM) has the task of gather information about devices neighbors, network conditions and communication statistics. Based on this info, the NM defines the routes used for communication. The evaluation of the routes used may help user to improve network performance and identify problems, as well as device characteristics.

Several works address the collection of diagnosis information for wireless networks, utilizing active and passive mechanisms [2, 6-7, 17-24]. Active mechanisms involve instrumentation of the network devices with monitoring software. Passive mechanisms utilize sniffers that overhear the packets exchanged on the physical layer [6]. The passive method has advantages, as no interference is added to the network. However, related works do not address specific issues about the passive monitoring of WH packets. WH utilizes an authentication/encryption mechanism to provide secure communication, so the tool must keep track of information to correctly decode the packets and obtain decrypted data. Commercial tools provide means for collecting and decoding WH packets, but the results are shown in a spreadsheet format, making the analysis of data a labor-intensive task.

This work discusses the development of a passive monitoring software tool for evaluation of topology and routes used in WH networks, with a specific architecture to deal with the security information of the protocol. The user can input collected log files or implement a communication directly with sniffers, allowing online and offline analysis methods. Once received, the packets are decoded, an overview of the network is built and by means of statistics, charts, lists, graphs, and other information about the network is shown, helping the user on different evaluations of the network.

The paper is structured as follows. Diagnosis approaches for wireless sensor networks are presented in Section 2. Section 3 presents a short brief of WH and the protocol packet structure and routing mechanisms. Section 4 presents the tool structure. Section 5 presents a case study using the tool in a WH network. The conclusion and the future works are presented in Section 6.

2 Related Work

The diagnosis of wireless networks can be achieved in an active or passive fashion. The active mechanism involves the instrumentation of the nodes with monitoring software for capturing of diagnostic information. The active approaches require nodes to transmit specific messages to diagnosis tools using the communication channel or

an alternative back channel [17-20]. This method may overload the normal network communication. A back channel is also not usually available on the devices and on the field. Scarce sensor resources (bandwidth, energy, constrained CPU and memory) may also affect the performance of this kind of diagnosis and change the behavior of the network [2]. The passive approaches in [2], [6], [21-24] utilize sniffers to overhear packets exchanged by the nodes, to form an overview of the network. This approach does not interfere on the network, as no additional bandwidth is required for diagnostic information transfer and no processing and energy power is used in the devices for diagnosis purposes [2]. On the other hand, the passive method is subjected to packet loss, caused by interference, collision and coverage of sniffers. Solutions for the sniffer's deployment problem are proposed in [22]. The hardware for the sniffers is not addressed in this work.

The software architectures for captured packets evaluation of IEEE 802.15.4 are proposed in [2], [6] and [24]. These works propose a generic architecture for collecting, merging, decoding, filtering and visualizing data. However, these approaches do not have mechanisms to deal with protocols that contain security and encryption like WH. Wi-Analys [7] is a commercial tool that provides means for collecting and decoding packets captured from WH networks, but the visualization of results is done in a spreadsheet format, what difficult the analysis of the information.

3 The *Wireless*HART Protocol

The WH standard is part of version 7 of the HART specification [8-9]. It features a secure network and operates on the 2.4 GHz ISM (Industrial, Scientific and Medical) radio band. The physical layer is based on the IEEE 802.15.4 standard in which direct sequence spread spectrum is employed [10]. A WH network supports a variety of devices, including field devices, adapters, portable devices, access points, network manager and a gateway to connect to a host application. The protocol allows multiple access and media arbitration by means of Time Division Multiple Access (TDMA) [11]. The links among devices are programmed and allocated in different time slots by the NM. The NM continuously adapts the routing and schedule due to changes in network topology and demand for communication [12]. The following subsections present the ISO/OSI layers of the protocol.

3.1 Data-Link Layer

The Data-Link Layer is responsible for secure, reliable, error free communication of data between WH devices [13]. The communications are performed in 10 ms timeslots, where two devices are assigned to communicate. A communication transaction within a slot supports the transmission of a Data-Link Protocol Data Unit (DLPDU) from a source, followed by an acknowledgment DLPDU by the addressed device. To enhance reliability, channel-hopping mechanism is combined with TDMA. DLPDU structure is presented in Fig. 1.

The CRC-16 ITU-T [14] is used for bit error detection and AES-CCM* [15] is used for message authentication. Authentication uses the WH Well-Known Key for advertisement DLPDUs and messages of joining devices. Other communications use the Network Key (provided by the NM when a device is joining the network). The Nonce used is a combination of the Absolute Slot Number (ASN) and the source address of the packet. ASN counts the total number of slots occurred since network's birth, and is known by devices through the advertise packets. Five types of DLPDU packets are defined: Advertisement, Acknowledge, Data, Keep-Alive and Disconnect.

Fig. 1. DLPDU structure

3.2 Network Layer

The Network Layer provides routing, end-to-end security and transport services. Data DLPDU packets contain in its payload a Network Layer Protocol Data Unit (NPDU), shown in Fig. 2. The NPDU contains three layers: Network Layer, with routing and packet time information, Security Layer that ensures private communication and enciphered payload, containing information being exchanged over network [16].

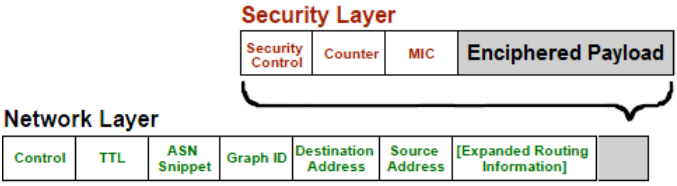

Fig. 2. NPDU structure

The AES-CCM* is also used for authentication of NPDU and decryption of the enciphered payload. The Join Key is used for devices joining the network. The Session Keys (provided by the NM when a device is joining the network) are used in other communications (between Device and Gateway, Device and NM). The Counter field of the Security Layer provides information for the Nonce reconstruction.

Three routing mechanisms are provided in the standard and are described below.

Graph Routing. A graph contains paths that connect different devices on the network. The NM is responsible for creating the graphs and configuring them on each device through transport layer commands [3]. A graph shows a set of direct links between source and final destination and can provide also redundant paths. To send a packet using this method, the source device of packet writes the specific Graph ID number in the NPDU header. All devices on the path must be preconfigured with graph information that specifies the neighbors to which packets may be forwarded.

Source Routing. The source routing provides one single directed path between source and destination device. A list of devices that the packet must travel is statically specified in the NPDU header of the packet [12]. This method does not require configuration of graphs and routes in the devices.

Superframe Routing. In this method, packets are assigned to a specific superframe and the device sends the message according to the identification of the superframe. The forwarding device selects the first available slot in the superframe, and sends the message. So, the superframe must have links that leads packet to its destination. Identification of the superframe routing is done in the NPDU header using the Graph ID field. If the field value is less than 255, then routing is done using superframe. If the value is 256 or more, then routing is done via graphs. A combination of superframe routing and the source routing is also allowed. In this case, the packet is forwarded through the source list with slots configured inside the specified superframe.

3.3 Transport Layer

The Transport Layer provides means to ensure end-end packet delivery, device status and one or more commands. Enciphered payload of the Security Layer contains a Transport Layer Protocol Data Unit (TPDU). Fig. 3 shows the structure of the TPDU packet.

Fig. 3. TPDU structure

4 Routing Monitoring Tool Structure

The structure of the proposed tool is presented in Fig. 4. The tool provides meanings for capturing and decoding captured data, obtaining network information and visualizing routes configured in the devices.

4.1 Capture

The capture of the packets exchanged by nodes is carried out in a passive way by installing one or more sniffers within the area of network. The sniffers add also a timestamp to the captured packets. The deployed sniffers may not be able to hear all packets that occur in network. Reasons involve radio sensitivity, positioning and noise. A partial coverage of the network can meet the requirements of some types of analysis for the WH protocol. This approach has the advantage of limiting the amount of data processed in later steps. Further information about sniffers deployment can be

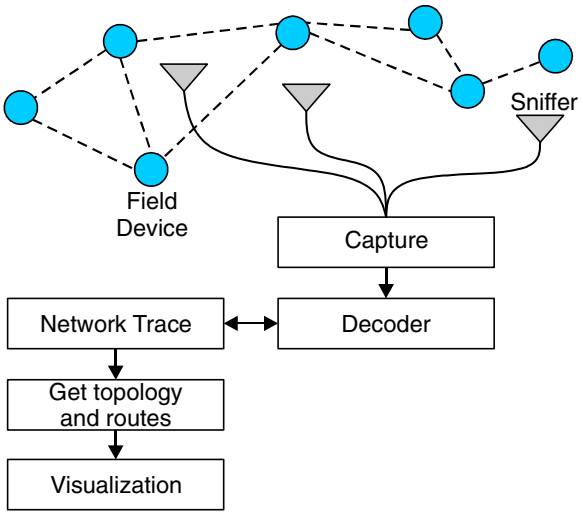

Fig. 4. Monitoring tool structure

found in [22]. For routing evaluation, sniffers may be deployed close to the Access Points, where all the management data to and from NM passes by.

An important factor to be observed in the diagnostic of WH protocol is the communication on multiple channels [13], requiring sniffers to be able to monitor the 16 channels simultaneously. Other issue is that the use of multiple sniffers introduces the need of a synchronization mechanism, since packets may be overheard in different sniffers who have a slightly different clock [2]. A merging process is necessary to combine several sniffers captures in a single trace, ordered according to the timestamp of packets. The merging methods can be found in [2], [6], and [21].

In order to keep the flexibility of the tool, the Capture Block has an interface for input of data from different sources, such as simulators, capture log files, or direct connection with sniffers. The received data is added in a queue to be processed.

4.2 Decoder

The Decoder Block aims to convert a packet from raw bytes to structured message description, according to the ISO/OSI model of WH. At the end of this process, the contents of the packets are interpreted to get information about network conditions. The decoding process is complex due the AES-CCM*, which requires that information about the keys and counters are obtained and stored. The main blocks of the decoder are shown in Fig. 5 and described below. Before execution, user must provide the system with the Network ID and Join Key to enable the decoder to obtain information needed for further authentication and decryption.

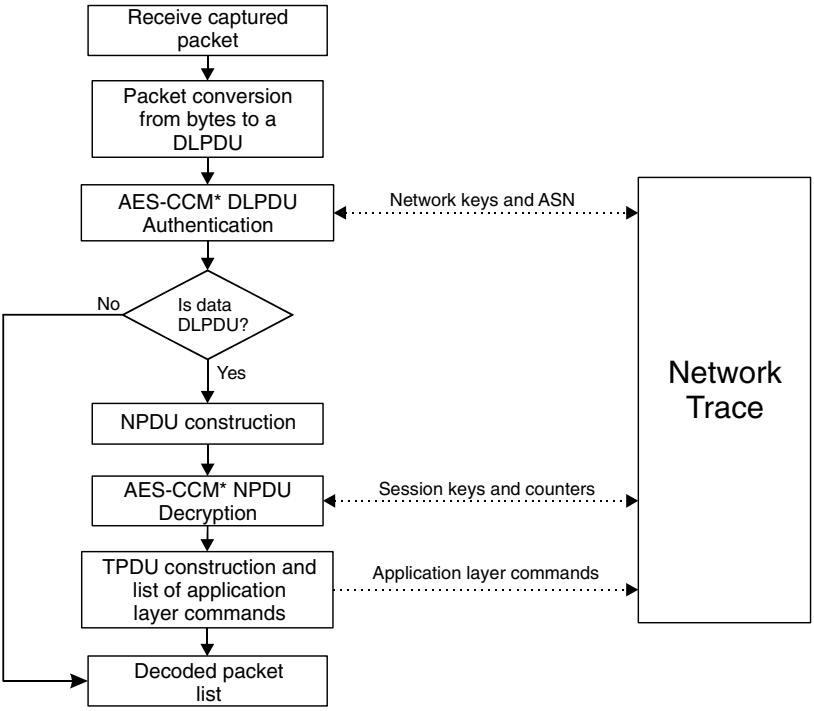

Fig. 5. Packet decoding sequence

Initially, the raw bytes of the packet are converted to its specific type of DLPDU. The packets with wrong CRC-16 and wrong header are identified. Once structured, the DLPDU packets that do not belong to the Network ID provided are identified.

Network Trace. The Network Trace Block provides the necessary information to the decoder for authentication and decryption of packets. It also holds information discovered of the network (e.g. devices, superframes and links). Depending on the coverage of the sniffers, the data stored in the Network Trace may be similar to the data stored in the NM, which have full information about the network operation. For each new message authenticated or decrypted, the Network Trace must be updated in order to maintain updated information of the keys, counters and network. Authentication and decryption of some packets may be compromised, as result of missing keys due to packet loss. The user should be aware of this issue when evaluating the network.

For authenticating the DLPDUs, the Network Trace must keep trace of the current ASN of the network, using an advertise packet captured. While the ASN of the network is not provided, authentication and further processes are compromised. The DLPDU must be authenticated in order to verify its integrity. The Message Integrity Code (MIC) field of the DLPDU is compared with the MIC obtained applying the AES-CCM* algorithm on the raw bytes of the DLPDU. The Network Trace Block

keeps track of the Well-Known Key and the Network Key. The Network Key is obtained during the join process of a device.

Once authenticated, the Network Trace is updated with the last ASN used and with the packet timestamp. The Data DLPDUs are decoded on the NPDU layer, while the other types of DLPDUs are sent to the Fill Message block. Another issue involves the decryption of the NPDUs. To do the decryption, sniffers must hear the join process of the device, where the Session Keys provided by the NM are obtained. Without these keys the system is not able to decrypt the contents of the Security Layer messages. For Data DLPDUs, the payload contained in the Security Layer of the NPDU is decrypted, using the Join Key or the specific Device's Session Keys and Session Counters.

Once decrypted, the packet is decoded in the transport layer, where a TPDU is generated. The Network Trace interprets the commands contained in the TPDU in order to maintain an updated view of the network, with Network Keys, Sessions, Superframes, Links, Device's Timers, Services, and further information. A list of all decoded packets is generated in order to allow filtering of messages in future applications of the tool.

4.3 Topology and Routes

The information discovered and stored in Network Trace is used to build an updated view of the network topology and the routes used. Network neighbor's information is used to build the topology of the network. The routes used for packet propagation are obtained based on the graphs, superframes and routes configured on each device. A graph representing each route is built for further analysis.

4.4 Visualizer

The topology and the discovered routes are summarized by the Visualizer Block to be easily interpreted by the user. Representations such statistics, charts and graphs can be used for analysis. Information contained in the Network Trace about the devices and network also may be displayed.

5 Case Study

In order to evaluate the tool, we deployed a WH network in a laboratory environment. The network consisted of the following devices: a Network Manager, an Access Point and a Gateway (Emerson model 1420A), nine WH-compatible field devices developed in previous work [26] and a Wi-Analys Network Analyzer Sniffer, from Hart Communication Foundation. Fig. 6a shows the WH-compatible devices and Fig. 6b the sniffer.

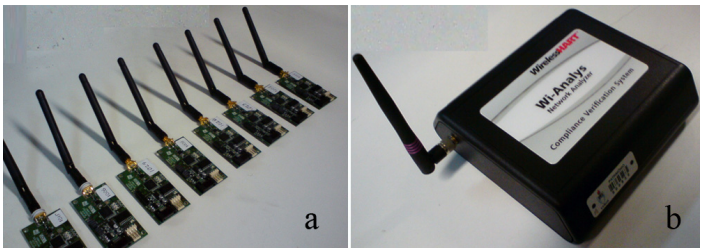

Fig. 6. WH compatible devices (a) and sniffer (b)

The data collected from sniffer was stored in a log file and later loaded in the tool. Packets were captured during a period of 120 minutes since network's birth. The sniffer was deployed close to the access point to get overall information of network. Fig. 7 shows a representation of the network.

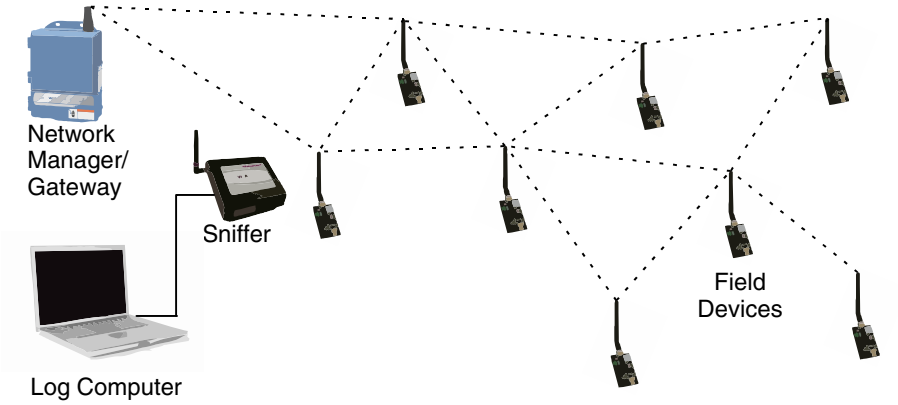

Fig. 7. Deployed network representation

The following subsections present analysis of the network behavior obtained with the captured packets. Before loading the file in the developed tool, we provided the Join Key (0x12345678000000000000000000000000) and Network ID (0001) of devices. The sensor devices publish their process variable each minute.

5.1 Network Topology Evaluation

The current topology of network is evaluated to find devices that may be bottlenecks for transferring data and devices with weak connections to neighbors. A graph is built showing discovered neighbors and the Received Signal Level (RSL) of packets overheard from neighbors. Fig. 8 shows the current graph when analysis reaches the end of log file. As observed, the connectivity of the network is high, as devices can hear almost all other neighbors. Blue circle represents the Access Point of the network.

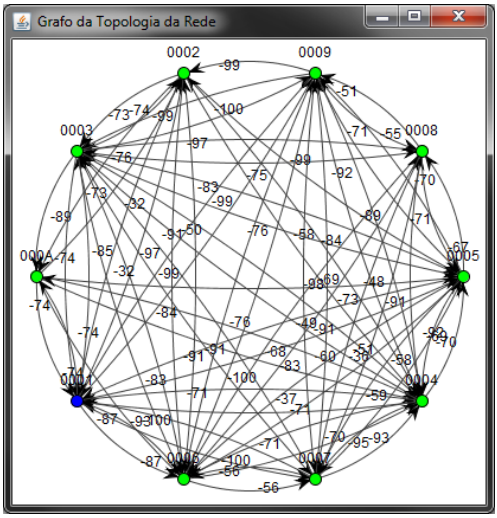

Fig. 8. Network topology graph

5.2 Routes used for Devices to Propagate Data to Access Point

The routes configured in the devices were used as basis to reconstruct information of graphs and paths of the network. Based on the information stored in the Network Trace, our tool has identified that the NM uses superframe routing. Superframe 0 has the uplink graph [3], used to forward data towards the access point. Superframe 1 contains the broadcast graph that is used by NM to send packets to all devices through a combination of source routing and superframe routing.

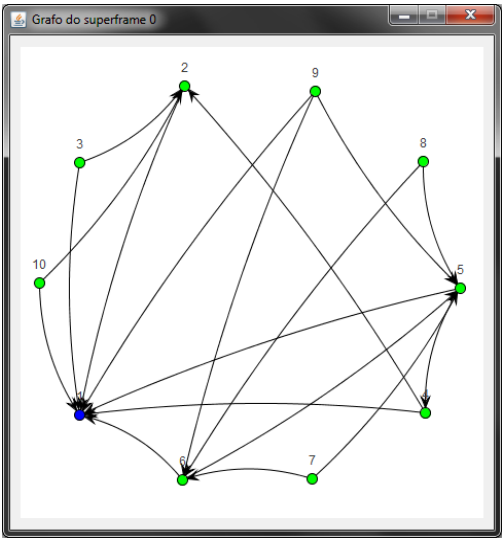

Fig. 9. Uplink graph contained in Superframe 0

6 Conclusion and Future Work

The use of wireless networks in industrial control and monitoring applications can present performance problems due to several factors. To track down such problems, it is necessary to inspect the network and nodes conditions after the deployment.

In this paper we present a software tool for inspection of routing in WH networks. Capture of information is done in a passive way by sniffers. The captured packets are used to build an overview of network topology and routes used in communications. Visualization of obtained information is done via graphs, charts and lists.

The study case has shown that tool can provide important information about the network conditions, and can help user to identify problems and understand the protocol and devices characteristics. User must be aware that packet loss caused by sniffers may affect the analysis.

On ongoing work, we are using this tool to analyze a WH deployment in an industrial application, to verify different aspects of network topology and routing strategies used in WH equipment. Information analyzed shall be used for improvements on devices and on Network Manager routing and scheduling algorithms, to better adjust the network performance for desired applications. The developing of enhanced algorithms for routing and scheduling in *Wireless*HART networks is still a necessity.

References

1. Tateson, J., Roadknight, C., Gonzalez, A., Khan, T., Fitz, S., Henning, I., Boyd, N., Vincent, C., Marshall, I.: Real World Issues in Deploying a Wireless Sensor Network for Oceanography. In: Proceedings of Workshop on Real-World Wireless Sensor Networks (REALWSN 2005), Stockholm (2005)
2. Ringwald, M., Römer, K.: Deployment of Sensor Networks: Problems and Passive Inspection. In: Proceedings of the 5th Workshop on Intelligent Solutions in Embedded Systems (WISES 2007), Madrid, pp. 180–193 (2007)
3. Han, S., Zhu, X., Mok, A.K., Chen, D., Nixon, M.: Reliable and Real-Time Communication in Industrial Wireless Mesh Networks. In: Proceedings of 17th IEEE Real-Time and Embedded Technology and Applications Symposium (RTAS 2011), Chicago, pp. 3–12 (2011)
4. HART Communication Foundation, `http://www.hartcomm.org/protocol/wihart/wireless_technology.html` (accessed September 2012)
5. Winter, J.M., Lima, C., Muller, I., Pereira, C.E., Netto, J.C.: WirelessHART Routing Analysis Software. In: Computing System Engineering Brazilian Symposium (SBESC 2011), Florianopolis, pp. 96–98 (2011)
6. Yu, D.: DiF: A Diagnosis Framework for Wireless Sensor Networks. In: IEEE Conference on Computer Communications (INFOCOM 2010), San Diego, pp. 1–5 (2010)
7. Han, S., Song, J., Zhu, X., Mok, A.K., Chen, D., Nixon, M., Pratt, W., Gondhalekar, V.: Wi-HTest: Compliance Test Suite for Diagnosing Devices in Real-Time WirelessHART Network. In: Real-Time and Embedded Technology and Applications Symposium (RTAS 2009), San Francisco, pp. 327–336 (2009)

8. Kim, A.N., Hekland, F., Petersen, S., Doyle, P.: When HART Goes Wireless: Understanding and Implementing the WirelessHART Standard. In: IEEE International Conference on Emerging Technologies and Factory Automation, Hamburg, pp. 899–907 (2008)
9. Song, J., Mok, A.K., Chen, D., Nixon, M., Blevins, T., Wojsznis, W.: Improving pid control with unreliable communications. In: ISA EXPO Technical Confererence, Houston (2006)
10. IEEE 802.11, http://grouper.ieee.org/groups/802/11/ (accessed July 2012)
11. Rappaport, T.S.: Wireless Communications – Principles & Practice. Prentice Hall Communications Engineering and Emerging Technologies Series, New York (1996)
12. Chen, D., Nixon, M., Mok, A.: WirelessHART: real-time mesh network for industrial automation. Springer, England (2010)
13. HART Communication Foundation, HCF SPEC 075, Rev. 1.1 (2008)
14. Simpson, W.: http://www.faqs.org/rfcs/rfc1549.html (accessed July 2012)
15. Dworkin, M.: Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality. National Institute of Standards and Technology. Special Publication 800-38C (2004)
16. HART Communication Foundation, HCF SPEC 085, Rev. 1.2. (2009)
17. Srinvasan, K., Kazandjieva, M.A., Jain, M., Kim, E., Levis, P.: SWAT: Enabling Wireless Network Measurements. In: ACM 8th Conference on Embedded Networked Systems (SENSYS 2008), Raleigh (2008)
18. Maerien, J., Agten, P., Huygens, C., Joosen, W.: FAMoS: A Flexible Active Monitoring Service for Wireless Sensor Networks. In: Göschka, K.M., Haridi, S. (eds.) DAIS 2012. LNCS, vol. 7272, pp. 104–117. Springer, Heidelberg (2012)
19. Rost, S., Balakrishnan, H.M.: A Health Monitoring System for Wireless Sensor Networks. In: Sensor and Ad Hoc Communications and Networks (SECON 2006), pp. 575–584 (2006)
20. Ramanathan, N., Kohler, E., Girod, L., Estrin, D.: Sympathy: a debugging system for sensor networks. In: IEEE 29th Annual International Conference on Local Computer Networks, Tampa, pp. 554–555 (2004)
21. Chen, B.-R., Peterson, G., Mainland, G., Welsh, M.: LiveNet: Using Passive Monitoring to Reconstruct Sensor Network Dynamics. In: Nikoletseas, S.E., Chlebus, B.S., Johnson, D.B., Krishnamachari, B. (eds.) DCOSS 2008. LNCS, vol. 5067, pp. 79–98. Springer, Heidelberg (2008)
22. Zeng, W., Chen, X., Kim, Y.A., Bu, Z., Wei, W., Wang, B., Shi, Z.J.: Delay monitoring for wireless sensor networks: An architecture using air sniffers. In: IEEE Conference on Military Communications (MILCOM 2009), Boston, pp. 1–8 (2009)
23. Depari, A., Ferrari, P., Flammini, A., Lancellotti, M., Marioli, D., Rinaldi, S., Sisinni, E.: Design and performance evaluation of a distributed WirelessHART sniffer based on IEEE1588. In: International Symposium on Precision Clock Synchronization for Measurement, Control and Communication (ISPCS 2009), Brescia, pp. 1–6 (2009)
24. Ban, S.J., Cho, H., Lee, C.W., Kim, S.W.: Implementation of IEEE 802.15.4 Packet Analyzer. In: International Conference on Computer, Electrical, and Systems Science, and Engineering (CESSE 2007), Bangkok, pp. 346–349 (2007)
25. Choong, L.: Multi-Channel IEEE 802.15.4 Packet Capture Using Software Defined Radio. M.S. thesis, UCLA (2009)
26. Muller, I., Pereira, C.E., Netto, J.C., Fabris, E.C., Algayer, R.: Development of WirelessHART Compatible Field Devices. In: IEEE Instrumentation and Measurement Technology Conference, Austin, pp. 1430–1434 (2010)