Preprints of the 19th World Congress
The International Federation of Automatic Control
Cape Town, South Africa. August 24-29, 2014

Towards a *Wireless*HART Network with Spectrum Sensing

Jean Michel Winter, Ivan Muller,
Carlos Eduardo Pereira
Department of Electrical Engineering
Federal University of Rio Grande do Sul
Porto Alegre, Brazil
{jean.winter, ivan.muller}@ufrgs.br, cpereira@ece.ufrgs.br

João C. Netto
Institute of Informatics
Federal University of Rio Grande do Sul
Porto Alegre, Brazil
netto@inf.ufrgs.br

Abstract—**The use of wireless communication systems for critical applications in a shared medium presents a lot of challenges regarding its reliability and robustness. The *Wireless*HART protocol, although robust has a lack of active mechanisms for coexistence, becoming vulnerable for interference sources. This paper proposes an expansion of the *Wireless*HART coexistence mechanisms, allowing an online analysis of the spectrum occupation and enabling new metrics for the selection of channels used by this protocol.**

Keywords— WirelessHART; spectrum sensing; energy detection; automation systems.

I. INTRODUCTION

Flexibility, mobility, expansion capability, maintenance and installation with reduced costs are the main advantages of wireless networks. Nevertheless, there are several challenges in wireless networks usage. These are related to the shared medium and radio frequency propagation phenomena such as, multipath signal reflections, low signal strength and interference, which may decrease the communication quality. To overpass these characteristics a robust and reliable protocol must be used, especially for applications that demand determinism and high reliability requirements. Some wireless protocols are already available for industrial applications, such as ISA SP100.11a and *Wireless*HART (WH).

WH is the first wireless protocol to be certified by the International Electrotechnical Commission (IEC) for industrial applications and has a set of characteristics to provide robustness, such as TDMA medium access, channel hopping, clear channel assessment, channel black listing, direct sequence spread spectrum, mesh network topology, and low duty cycle. Although these characteristics, there are studies in the literature that describe loss of performance on WH under interference circumstances [1][2] [3].

Handling with coexistence is a big challenge in wireless networks. Usually it is necessary and recommended to realize a wireless site survey to evaluate environment conditions. This process is usually performed before devices installation. A site survey can identify sources of interference and estimate a proper radio deployment. However, these services usually involve high costs and the results are related just for the RF picture at the moment of analysis. It has no efficiency against eventual interferences provided by mobile devices or even a new network to be installed. Currently, the available standards do not handle the problem of possible coexistence with other protocols (are inherently "selfish") and do not have mechanisms to discover and effectively co-exist with other devices using different solutions [1]. WH standard follows the same direction and its mechanisms can be classified as passive methods, once they run independently from the environment changes. This lack of reaction leads to a research gap for improving its robustness.

In this work it is proposed for the WH standard an online mechanism for assessing the spectrum occupation, thus providing means for the protocol to react and mitigate problems caused by coexistence issues. This work is structured as follows: section II introduces the WH protocol. Section III presents some general aspects concerning spectrum sensing. Section IV presents an analysis of a practical WH network, and Section V presents a WH spectrum sensing proposal.

II. THE *WIRELESS*HART PROTOCOL

The WH protocol is the seventh version of the HART protocol and it incorporates wireless functions. The HART protocol was launched in the 80's and it is widely used in the industry. On the application layer both versions of the protocol share the same features. At the physical layer, according to the OSI model, WH protocol is based on the IEEE 802.15.4 standard [4], operating within the 15 channels of 2.4 GHz ISM band (see Fig. 1). The network uses mesh topologies, with no hierarchy between field devices, each device on the network can act as router to the messages reach the final destination.. The topologies are dynamically created by the NM, which is based in some metrics and different occurrences such as, receive signal strength, number of devices, neighbors, etc. WH is a self organizing and self healing network presenting features such as channel hopping and different routing strategies in order to increase reliability.

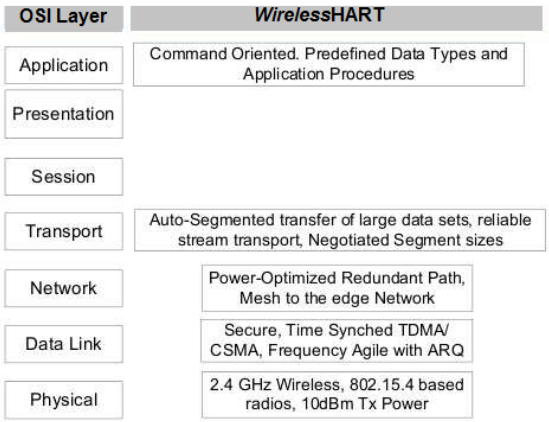

Figure. 1. WirelessHART and OSI model [6].

Fig. 2 shows a typical WH network with its fundamental components: network manager (NM), security manager (SM) and access point (AP), which are mandatory and usually reside inside one box. The WH components are described below:

- Network manager, responsible for network configuration, managing messages routes, and monitoring network health;
- Field devices perform basic functions of sensing and actuation in the plant. WH field devices have the ability to forward messages from other field devices towards the gateway;
- Adapters allow legacy wired HART to be used within wireless communications;
- Portable devices are used for calibration, commissioning and inspections;
- Access points that connect the field devices with a gateway;
- Gateway, which enable communication between the access point, network manager, security manager and the host application.

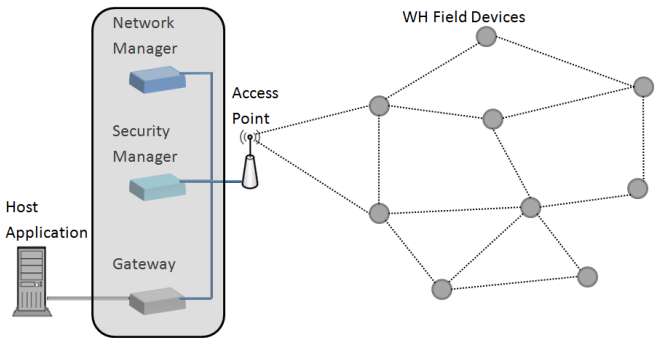

Figure. 2. Typical WH network.

III. RF SPECTRUM SENSING

Being aware for the frequency spectrum occupancy and the existence of users in the used bands is the main goal of sensing spectrum (SS). Traditional SS can be understood as a measure of the content or the measurement of radio frequency energy in the spectrum. In literature, the term spectral sensing is often attributed to the concept of cognitive radio, and it has a more general understood, obtaining the spectrum characteristics of users in different dimensions (space, time, frequency, and code). This includes the identification of what types of signals are being used, such as modulation type, waveform, bandwidth, etc. The cognitive radio researches introduce different strategies to share the communication resources. In [5] and [6] are presented different spectrum sensing methods, and they are listed below:

- Energy detection (ED): This is a basic spectrum sensing technique. It measures the received energy during a period of time. It requires low computational and implementation resources. Usually it is implemented with a threshold signal to distinguish the noise floor from the real interference source. It is not able to differentiate modulated signals from noise and interference;
- Cyclostationary: This method explores the periodicity or statistical characteristics of a signal, such as carriers, pulse trains, repeating spreading, hoping sequences, etc. Cliclostationary detection algorithms are able to differentiate signals from noise, once the noises are usually stationary [5];
- Matched-Filtering: This is a powerful method and it is able to maximize signal to noise ratio. But, it requires a previous knowledge of the interfering signal (PHY layer). Such information must be available to the radio. Another drawback is that the radio need a dedicated receiver for every class of radio signal [7] ;
- Waveform Based Sensing: It requires short measurement time and it is based in the detection of the signal patterns to assist synchronization, such as, preambles, spreading sequences, regularly transmitted patterns, etc. It is an efficient method, but also requires a knowledge regarding the signal patterns;
- Radio Identification: This method has to extract several features from the received signal and classify which technology is being used. However to process all of this information, requires a set of combined methods such as ED, neural networks algorithms, and thus, it becomes a complex method for radio identification.

Although the different mechanisms presented in literature, a multi-dimensional radio spectrum sensing space requires special hardware with high sampling rate, high resolution from analog to digital converters, high speed signal processors and in some cases, a previous knowledge of the radio patterns [6]. Fig. 3, illustrates a relation between complexity and accuracy of the discussed methods.

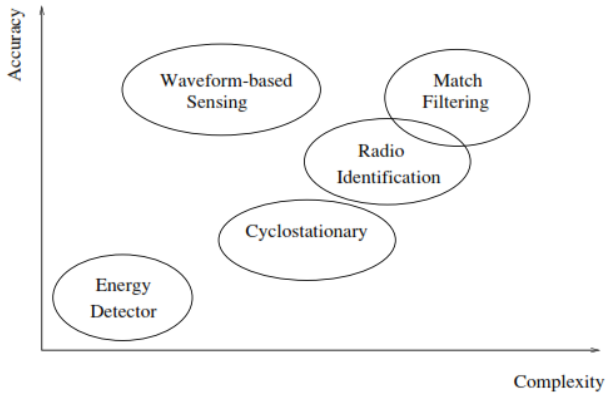

Figure 3. Main RF spectrum sensing methods (accuracy versus complexity). [5].

IV. *WIRELESS*HART SPECTRUM SENSING PROPOSAL

Industrial, Scientific and Medical (ISM) radio bands are defined by the ITU- R (International Telecommunication Union – Radio communication), and are internationally reserved for scientific, medical, and industrial purposes. Among the many established radio bands the 2.4 GHz band is widely used because of worldwide availability. The interest for the use of this band has grown in low power and short range communication systems, being stimulated by several factors, such as no need of licensing which ends up being a great economic attractive. Many communication standards like Bluetooth, ZigBee, WiFi, WH, WIA-PA, ISA 100.11a and others. Although these systems present many differences (band width, transmission, modulation techniques, synchronization headers, etc.), there may be interference between them. The 2.4 GHz band usage demand brings serious concerns regarding the robustness of these protocols when under coexistence situations.

A. Spectrum use by the WirelessHART

The WH standard uses black channel listing, allowing channels to be rejected from the WH network. This option allows interference rejection, especially for stationary interferences or narrow band sources. This option brings benefit for communication reliability, presenting a solution for WH communication in relation to permanent interference. These are possible to occur, especially when coexisting with WLAN networks, which could be avoided since WH band is relatively narrow. This mechanism avoids paradox situations in which traditional IEEE 802.15.4 networks, using only a fix channel far away from the stationary interference source could have a better performance than a WH network, that crosses this region in some time slots [1], (through channel hopping), see Fig. 4.

An important aspect of this mechanism is the fact the adjustment of the channels selection by the network planner is necessary because the black channel listing is not a self-adaptive mechanism. The analysis of the spectrum availability must be made previously through a site survey. Then it may be possible to determine interfering frequency bands and to identify the best channels for use in the regular communication. A further drawback is the necessity to restart the network for each new channel list, since the channel map is transmitted only when the device is joining to the network. The advertise DLPDU provides basic network information, such as absolute slot number (ASN), join control information, security levels supported by the network and channel map array [8]. The channel map array is used to determine the channel hop sequence during the network communications.

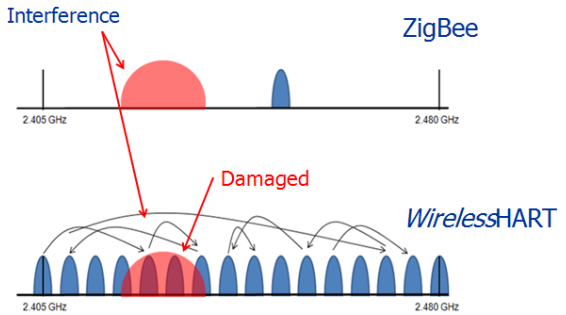

Figure 4. Protocol with channel hopping and protocol with a fix channel under a stationary interference.

WH uses the superframe concept in the communications. A superframe consists of a set of fixed time slots. The typical slot when allocated within the superframe has a set of characteristics. The superframes are created and maintained by the NM which adds, deletes and modifies the links. Each link belongs to only one superframe and they are distributed into a superframe by the NM. The link includes a reference to a neighbor and defines a communication opportunity (see Fig. 5). The type of link determines whether it is use for communication between peer devices or to a broadcast propagation.

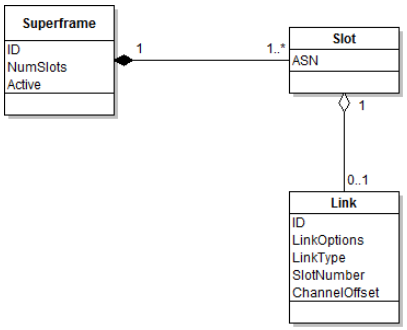

Figure 5. Superframe and link relationship. (Adapted from [8]).

The link specifies the channel offset and this parameter is also responsible for channel hopping order. In a given absolute slot with an active link, the actual channel that will be used is determined by (1).

$$ActiveChannel = \left(\frac{ChannelOffset+ASN}{Number\ of\ Active\ Channels}\right) \qquad (1)$$

The result of the equation is the channel that must be used for communication in a specific ASN. Each link is associated with a specific time slot in a specific frequency. The type of the destination determines the link type that can be used and consequently the appropriate slot for the DLPDU. There are four types of links: Normal, Discovery, Broadcast and Join [9].

- Normal: It is the most common link. It has a source and a destination address;

- Discovery: It is a link to maintain connectivity among the devices and also to allow devices to discover new neighbors. Discovery links are also shared;
- Broadcast: This link is always associated with a time slot shared between all devices;
- Join: It is used during join period and has advertisement information with necessary parameters for a device to join the network. This links are shared because multiple joining device could send messages to a proxy device.

B. *WirelessHART Spectrum Analysis*

A practical WH network is deployed in a laboratory environment and an analysis regarding the spectrum frequency occupation is evaluated. A commercial gateway and a temperature sensor node are employed, as well as a set of field devices with a WH stack [10].

The WH allows adjusted some publication information, e.g. process variable, to be periodic published and available to process application. The burst publications are inherent of WH protocol and are configured according to the system requirements. To achieve temporal requirement given by the process, the NM must ensure sufficient resources for field devices to become apt to propagate their messages. This implies in a strict scheduling links control with timing precision and redundant possibilities in case of failures.

In the first analysis, the link list of field devices on the network are obtained and mapped. Table I, shows a set of distributed links for Device 1 on the test bed experiment. For each link, there are different attributions. For example, the index 0 link belongs to Superframe ID 1 and it is placed in the time slot number 212 with a channel offset equal to 2. The neighbor nickname for this link corresponds to 65535 (0xFFFF, it is a broadcast link), and it is a link designated to broadcast reception.

TABLE I. LINKS MAP FOR DEVICE 1.

Link Index	Superframe ID	Time Slot	CH Offset	Nickname	Option	Type
0	1	212	2	65535	RX	Broad
1	0	986	1	1	TX	Normal
2	0	1	0	1	TX/RX	Discovery
3	4	115	7	65535	TX	Broad
4	0	218	5	1	TX	Normal
5	1	230	1	63872	TX	Join
6	1	242	3	65535	RX	Broad
7	0	367	3	63872	RX	Join
8	0	474	5	1	TX	Normal
9	0	730	3	1	TX	Normal
10	0	346	2	1	TX	Normal

In this network one can observe that the NM is using at least 3 superframes (superframes ID 0, 1 and 4). In this case, the superframe of interest is superframe ID 0, which DLPDUs from Command and Data type are sent and received. Fig. 6 illustrates only the Normal link types from two devices with its channel offset and the position in the superframe.

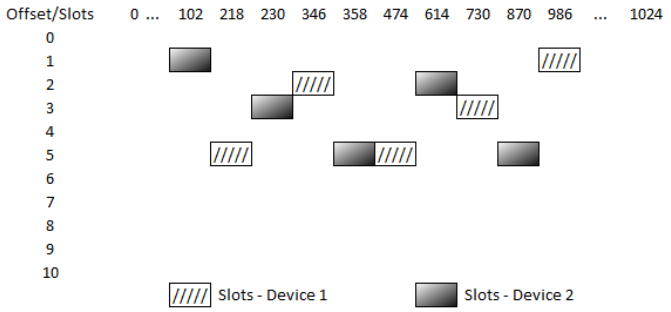

Figure 6. Time slots distribution in the superframe with Transmit Links from two devices on the network.

In the adopted strategy, field devices received the same temporal requirements for the process variable publication. The process variable publication occurs every 4 seconds. The superframe ID 0 has 1024 time slots, meaning a 10.24 seconds duration. Through network analysis, it can be highlighted:

- Programmed devices have 5 time slots available for transmission of the primary variable, with minimum spacing of 128 ms and a maximum of 1280 ms. This represents at least four opportunities to send the primary variable value, in order to guarantee network determinism;
- It is observed that the management policy adopted by the NM, distributes alternative connections that precede the deadline for the variable publication. Each connection uses a different frequency channel. If a collision occurs in one of the transmissions, there is another possibility, in a different scheduled link.

In a second analysis the burst time of a particular device is tested for different time requirements, and through a software developed in previous work [11], the distribution of the links from our target device were obtained and monitored. It is possible to observe the NM efforts to allow sufficient opportunity for the device to be able to fit the deadline specified in the application.

Fig. 7 illustrates how a sequence of links is distributed to a specific device. In this experiment, it is noticed the demand for redundant links. It was set up different Burst time requirements and registered the number of links assigned to the target device. For simplification purposes, Fig. 8 presents just links of Normal type and Transmit option, in this case with a superframe size of 1024 slots. The number in the box (e.g. 34, 286, 429 and 795) represents the position of the link in the superframe. In the first situation a deadline for 32 and 16 seconds was adjusted and the NM assigned 4 slots inside a period of 10,24 s, it means that for a period of 32 seconds there are at least 12 opportunities to send the packet without extrapolating the deadline, see Fig. 8. Thus, there are 12 exclusive slots for a unique device on the network.

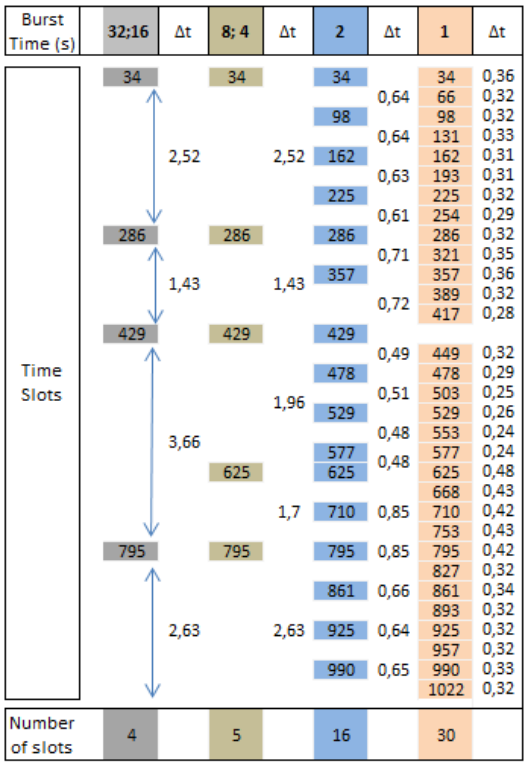

Figure 7. Time slots assigned for different burst time requirements.

Fig. 8, illustrates a superframe with 1024 time slots and the Transmit links (Normal type) distribution. It is possible notice the redundant links.

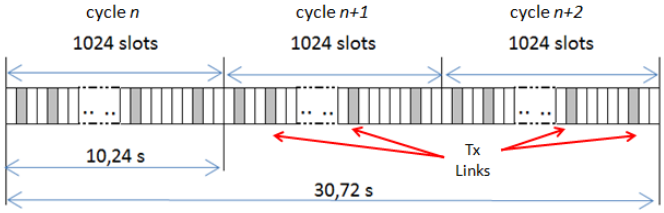

Figure 8. Superframe cycle with Transmit Links.

C. *WirelessHART Spectrum Sensing Proposal*

This session presents a proposal to best employ the not used redundant transmit links in a superframe cycle. The physical layer of IEEE 802.15.4 has two functions to measure and indicate the level of interference within a frequency channel. The measured power at the receiver, LQI (Link Quality Indication), is an estimate of the received signal strength on a channel and is applied for a received packet. The Energy Detection function is a mechanism to measure power within an IEEE 802.15.4 channel. The ED function does not require spectrum information from others users, also it doesn't require any transmitted signal properties. The ED method, is also described as radiometry or periodogram and is the most generic and common way of spectrum sensing.

A traditional medium access mechanism in the literature and available in the IEEE 802.15.4 standard which is also based on ED method, is the Clear Channel Assessment (CCA). In IEEE 802.15.4, CCA classifies a channel in busy or idle through a scan period of 128μs, which precedes a message transmission. Several studies [12][13][14] show that even this mechanism with low complexity brings many gains in reducing interference and packet losses.

In this work the ED mechanism is chosen for the spectrum analysis, once it is already incorporated on IEEE 8002.15.4 radios and its advantage of low complexities characteristics. Differently from the CCA method, it is proposed a period of ED scan equal to the WH time slot, it corresponds approximately to 10 ms (78 times larger). For the detection of energy occurs at the proper time and frequency is proposed a change in the TDMA state machine implemented by the WH protocol, see Fig. 9. Originally it employs six states: Join, Talk, Wait for Ack, Listen, Answer and Idle, there are a brief description about them above:

- Join: when a new device is attempting to join the network, it receives a list of superframes, graphs and links;
- Talk: this state is entered when an event indicates that a slot needs to be serviced (slot time out) with a transmit link;
- Wait for Ack: this state occurs after the occurrence of the Talk state and the device sends a no broadcast message ;
- Listen: the Listen state is entered if an event indicates that a slot needs to be serviced with a receive link;
- Answer: if a packet is captured then the state Answer is entered;
- Idle: when is in no other state, the device stays on Idle mode and managed the different events, such as Slot Timeout, Flush.request, Transmit.request and events to schedule new links and superframes.

It is proposed an addition of a seventh state, called here, Spectrum Sensing state, which it is responsible for execute the energy detection function for specific time slots. As it was demonstrated in the preceding analysis it is intended to use the empty transmit links available in the device by circumstances of reliability, but without demand, once the communications are successful. The state is entered when a transmit slot occurs (Transmit link's type) and there is no pending packet to be sent (Tx Queue is empty), so the spectrum sensing function can attempt to scan and measure the channel logically in use.

An ED scan allows a device to obtain a measure of the energy in each requested channel, as this function is programmed to occur in a reserved slot no messages are discarded and there is the guarantee that no one device from the same network is inserting energy on the channel. This approach becomes the classification channels easier for the channel select algorithms in a next step.

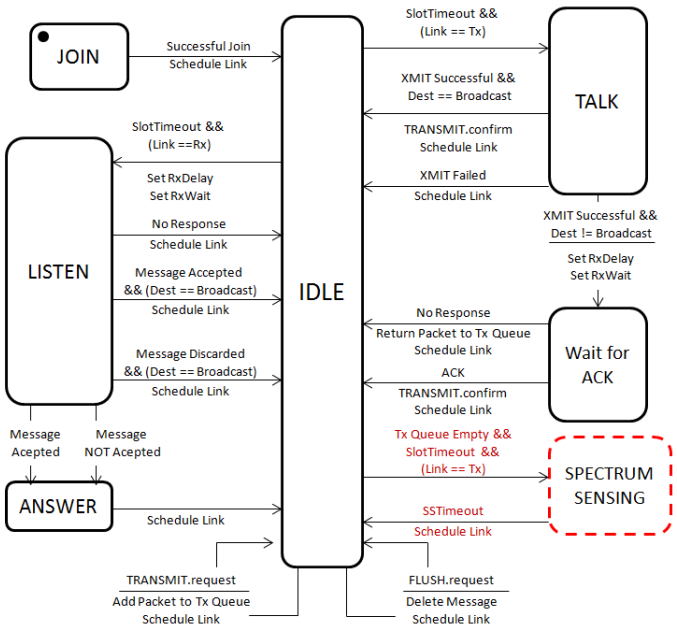

Figura 9. TDMA state machine proposal.

One of the great advantages of this sensing strategy is its computationally feasibility in real time. Allowing a fast diagnose of the spectrum without interfere or change the communications integrity of the WH network. At least three important information about the resources are identified: time, frequency and energy level. With these metrics available and an appropriate channel classification algorithm may be possible mitigate or prevent damages caused by interference in communications, so as to avoid the frequency bands with high levels of interference.

CONCLUSIONS

This work presented an analysis of the distribution of resources (time and frequency) on a WH network. Although the WH has shown to be a robust protocol, it was identified situations in which there is great demand for network resources which are underutilized and also becomes clear the lack of dynamism of the protocol to explore free band in the 2.4 GHz spectrum as well to avoid occupied channels with interference sources .

A mechanism is proposed to integrate into the WH for online spectrum sensing at the channels used by the protocol. The proposed strategy allows each device to be aware about the resources distribution in the network and performs the spectrum scan in unique temporal opportunities with the guarantee of non-occurrence of any other signal from the same WH network. This feature brings great vantages for identifying interfering sources through a sensing method of low complexity, once there is no necessity to distinguish interference signal from signals provided by its own network.

A further step in this work is to define an algorithm for link quality classification into the channels used by the protocol and thus allow a reduction in the packet loss due to interference sources, further enhancing the reliability of the WH protocol.

ACKNOWLEDGMENT

We would like to express our gratitude to CNPq and Capes, our governmental commissions for post graduation and research on their support for this work.

REFERENCES

[1] De Dominicis, C. M., et al. "Investigating WirelessHART coexistence issues through a specifically designed simulator." Instrumentation and Measurement Technology Conference, 2009. I2MTC'09. IEEE. IEEE, 2009.

[2] Petersen, Stig, et al. "Requirements, drivers and analysis of wireless sensor network solutions for the Oil & Gas industry." Emerging Technologies and Factory Automation, 2007. ETFA. IEEE Conference on. IEEE, 2007.

[3] Winter, J. M. "Análise de Coexistencia em Redes WirelessHART", dissertação de mestrado. UFRGS. 2013.

[4] IEEE 802.15.4, Institure of Electrial and Electronics Engineer. Part 15.4, Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs). New York: IEEE Computer Society, 2006.

[5] Yucek, Tevfik, and Huseyin Arslan. "A survey of spectrum sensing algorithms for cognitive radio applications." Communications Surveys & Tutorials, IEEE11.1 (2009): 116-130.

[6] Axell, Erik, et al. "Spectrum sensing for cognitive radio: State-of-the-art and recent advances." Signal Processing Magazine, IEEE 29.3 (2012): 101-116.

[7] Cabric, D.; Mishra, S.M.; Brodersen, R.W., "Implementation issues in spectrum sensing for cognitive radios," Signals, Systems and Computers, 2004. Conference Record of the Thirty-Eighth Asilomar Conference on , vol.1, no., pp.772,776 Vol.1, 7-10 Nov. 2004

[8] Hart Communication Foundation. HCF_SPEC-075, Rev. 1.1. Austin: HCF

[9] Chen, Deji, Mark Nixon, and Aloysius Mok. Why WirelessHART. Springer US, 2010.

[10] Muller, Ivan, et al. "Development of a WirelessHART compatible field device."Instrumentation and Measurement Technology Conference (I2MTC), 2010 IEEE. IEEE, 2010.

[11] Winter, Jean M., et al. "WirelessHART Routing Analysis Software."Computing System Engineering (SBESC), 2011 Brazilian Symposium on. IEEE, 2011.

[12] Zeghdoud, M.; Cordier, P.; Terre, M., "Impact of Clear Channel Assessment Mode on the Performance of ZigBee Operating in a WiFi Environment," Operator-Assisted (Wireless Mesh) Community Networks, 2006 1st Workshop on , vol., no., pp.1,8, Sept. 2006

[13] Ramachandran, I.; Roy, S., "WLC46-2: On the Impact of Clear Channel Assessment on MAC Performance," Global Telecommunications Conference, 2006. GLOBECOM '06. IEEE , vol., no., pp.1,5, Nov. 27 2006

[14] Soo Young Shin; Ramachandran, I.; Roy, S.; Wook-Hyun Kwon, "Cascaded Clear Channel Assessment: Enhanced Carrier Sensing for Cognitive Radios," Communications, 2007. ICC '07. IEEE International Conference on , vol., no., pp.6532,6537, 24-28 June 2007