DOI: 10.48011/asba.v2i1.1463

Method for Detecting Transmission Link Failure in Industrial Wireless Networks ⋆

Leomar M. Radke * **Gustavo Cainelli** * **Max Feldman** *
Carlos Eduardo Pereira * **João C. Netto** * **Ivan Müller** *

* *Universidade Federal do Rio Grande do Sul (UFRGS), Porto Alegre, Rio Grande do Sul, Brasil (e-mail: leomar@hotmail.com, gustavo.cainelli@gmail.com, max.feldman@ufrgs.br, cpereira@ece.ufrgs.br, netto@inf.ufrgs.br, ivan.muller@ufrgs.br).*

Abstract: Industrial Wireless Networks have been increasingly employed in industry. In many industrial environments device failures can occur. The detection of failures is essential for the proper network operation. This work aims to accomplish link failure detection in an Industrial Wireless Network. A link failure can occur if the radio Power Amplifier presents problems. If the power amplifier does not work properly, asymmetry may occur in communications since the Power Amplifier is responsible only for the transmission. It is proposed an algorithm which periodically analyses the Receive Signal Level of transmissions and infer whether happening a Power Amplifier fault in some device. The proposed method contributes to the correct diagnosis of network problems since link asymmetry can induce the Network Manager and also the user to understand that healthy devices are not working correctly.

Keywords: WirelessHART, Power Amplifier Failure, Transmission Failure, Link Failure.

1. INTRODUCTION

Industrial Wireless Networks (IWN) are an alternative to wired industrial communication. The main advantages of using this type of technology are mobility, cost reduction with cabling, installation, among others, see Müller et al. (2012). With the rapid advancement of IWN, several communication protocols were developed such as WirelessHART (WH), WIA - PA and ISA100.11a. Each protocol has its own characteristics, but all of them use the IEEE 802.15.4 standard on the physical layer, see Wang and Jiang (2016). The proposal presented by this work was developed using the WH protocol, although it can be applied to other protocols.

Another essential activity for the operation of the IWN is the constant evaluation of the network health by the Network Manager (NM). Therefore it is necessary that the diagnoses are accurate. Situations such as blockages, interference and even hardware failure can impact communications.

One kind of issue that significantly compromises the link is the device transmission power. This type of flaw may occur in a network due to two reasons: inadequate commissioning of transmission power or due to a flaw on the power amplifier (PA). The first is due to inadequate adjustment of Radio Frequency (RF) transmission power, which can occur both when commissioning and adjusting a field device already operational. The second is due to a possible PA hardware failure caused by the overheating resulting of the relative high level of power convertion in this component. These characteristics make the PA one of the most likely components to fail on a device. Some of the devices that are part of typical IWN are the NM, responsible for creating and maintaining the network, the Gateway, responsible for connect the network to the automation plant, the Network Access Point (NAP), and the field devices that are connected directly to the plant. In addition, applications can interact with the network through the gateway. Usually the devices in IWN have the ability to route packages characterizing the network topology as a mesh. Transmissions between devices occur through links where at least two links (TX and RX) exist between a pair of devices.

In Figure 1 transmission links are represented by the arrows that leave the device, and the receiving links are represented by the arrows that arrive at the device.

The PA is the component responsible for amplifying the transmission signals. A failure in the Power Amplifier of a device will lead to loss of power in radio transmission links. Figure 1 shows device 2 that fails PA. The dashed arrows represent reduced signal level from transmission links.Such a failure can lead to a misdiagnosis of the network. If the faulty device, in this example the FD2, is close enough to the NAP or other field devices, it is possible to remain

⋆ This study was financed in part by the Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Finance Code 001 and by the Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq). The authors would like to thank the Brazilian research agencies CAPES and CNPq for the financial support of this research.

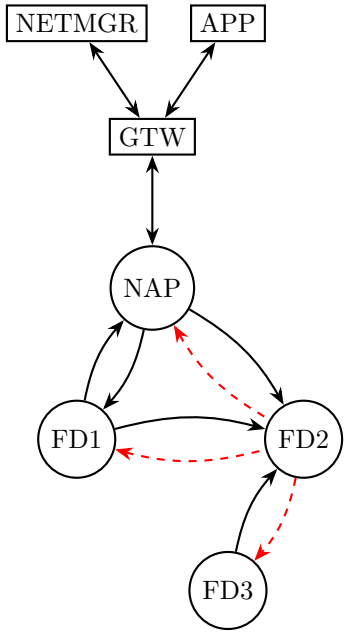

Figure 1. Topology of an IWN in which a field device (FD2) has failed its Power Amplifier

operational despite its low transmission signal level. One of the consequences of operating at reduced signal level is a possible increase in the number of packets lost in the network communications. In addition, if the problem device is between the NAP and another field device, in this example represented by FD3, a healthy device may stop receiving NAP packets because the link responsible for transmitting these messages is inoperative. This type of situation causes the NM to understand that FD3 is out of the network because the messages from the manager do not reach FD3, so it does not answer them. The fact that a device is off the network can lead to the maintenance technician to replace FD3 trying to solve the problem. In this way, it can be seen that without the correct diagnosis ineffective attempts to solve this network problem.

Considering the problems that a failure in the PA can lead to the IWN and the importance of the correct diagnosis, this paper presents a method to evaluate link failure in IWN transmissions, proposing the analysis and comparison of the signal levels of the transmissions between neighbors of a network in order to detect faults in the hardware of the field devices and provide correct diagnosis to network operators.

This work is organized as follows: the Section 2 presents some work related to the failure detection in IWN; Section 3 presents the theoretical basis as well as the description of the problem; Section 4 shows the operation of the algorithm proposed and testing methodology; In Section 5 the results; We conclude the discussion and visualize future works in the Section 6.

2. RELATED WORKS

Some works have analyzed hardware failures influence in IWN, see Kenyeres et al. (2011); Wang et al. (2018); Virkki et al. (2011); Silva et al. (2013); Maheswar and Jayaparvathy (2012). Other works propose tools to insert network failures and analyze the results. Some of them, like the one proposed by Kunzel et al. (2012) has a implementention of WH network inspection enviroment. The capture of information is done in a passive way using a sniffer to monitor the network. The tool, developed in the laboratory, presents the results through graphs and tables of metrics, which are used to evaluate the WH network.

In Machado et al. (2013) a tool for inspection and analysis of the network is proposed. The main advantage presented by the author is the mobility and inspection of all 15 channels of a WH network using only one radio. The system is capable of measuring the energy level in the 15 RF channels and produces information on the logical aspects of the links. In Machado et al. (2014) an extension is proposed where it is developed an offline application that presents several analyzes on the network data. The results show that the tool works similar to a multichannel sniffer detecting network interference.

In Nobre et al. (2014) an evaluation of the energy consumption and reliability in IWN with defective links is made using the NS-3 network simulator for the WH physical layer. The proposal includes the error model, devices positioning, signal attenuation and power consumption. Furthermore it is possible to configure each link with different failure probabilities, but only in simulated environments.

In order to evaluate a WH network in adverse situations caused by failures, Winter et al. (2016) uses a WH network, where the network is controlled to produce a specific scenario in which a failure can be inserted in the network. The study points out that failure leads to a misinterpretation of the state of the network, which is proven by experiments. Proposals to identify and solve problems are presented by the authors.

In Krötz (2019) a software tool is proposed to monitor and insert failures in IWN. The tool has several functionalities for the insertion of faults in the network, hence it is possible to evaluate the temporal behavior of both in normal operation and under fault conditions. The author also presents three case studies where the influence of failure in packet delivery latency are studied. In addition, the author reviews the works related to analysis and insertion of failures in IWN.

3. THEORETICAL FOUNDATION

This section presents some important concepts for the development of this work as well as the description of the problem to which the proposed method seeks to answer.

3.1 WirelessHART Protocol

The WH standard provides specification for physical, link, network, transport and application layers. WH networks are mesh networks, in which each device has the ability to route packets. The WH physical layer is a simplified subset of the IEEE 802.15.4 standard and uses the 2.4 GHz band divided into 15 channels, see Chen et al. (2010) Foundation (2007). The standard uses Time Division Multiple Access (TDMA) to provide collision-free and deterministic communications. The concept of superframe is presented as a sequence of consecutive timeslots, see Chen et al. (2010).

The data link layer provides reliable means for transferring data between the network nodes, detecting and possibly correcting errors that may occur at the physical layer. This layer has the important task of creating and managing data frames, see Chen et al. (2010) Foundation (2008a). The application layer of the WH protocol is command oriented. It is at the application layer that the HART commands are implemented, defining the types of data that must be loaded into the messages. Each command uniquely specifies the data packet and its size.

One of the key commands for maintaining the network is command 780 (Report Neighbor Health List). This is a Wireless Command which provides statistics for linked neighbors, see Foundation (2008b). Some of the information that the 780 command returns are: total number of neighbors; nickname of neighbor; mean RSL (Receive Signal Level) in dBm since last report; packets transmitted to this neighbor since last report; packets received from this neighbor since last report.

3.2 Received Signal Level

The RSL represents the signal power level that a device receive in a peer communication. Consequently, the higher the RSL, the stronger the received signal. It is important that devices constantly store statistics such as mean RSL, packets lost, last timestamp communication, among others, see Chen et al. (2010) Foundation (2008a).

The devices store statistics for each of its neighbors. The RSL is calculated using an Infinite Impulse Response (IIR) filter using (1).

$$RSL = RSL - \frac{RSL}{RSL_{Damp}} + \frac{RSL_{Measured}}{RSL_{Damp}} \qquad (1)$$

Periodically, a device sends health reports from its neighbors to the NM. The integrity value of the network is mainly the RSL of its neighbors. The RSL value is updated after each report, see Chen et al. (2010). This is a key metric for the methodology proposed in this work.

3.3 Power Amplifier

In this work, radios developed in Muller et al. (2010) were used. These devices use the integrated circuit CC2591. The CC2591 is a low-cost, high-performance RF front end for 2.4 GHz wireless, low power and low voltage. The component has a PA to increase output power and an LNA with low noise to improve receiver sensitivity, see Instruments (2014). Figure 2 shows the CC2591 eletric diagram. Both the transmission path and the receiving path use same antenna for communication, but the transmission passes through the PA and the reception do not. This is a typical RF front end interface.

3.4 Power Amplifier Failure

The case study that will be presented is motivated by the work of Winter et al. (2016); Krötz (2019). These authors studies and present some tools that contribute to the analysis of this type of technology under fault conditions. The author Winter et al. (2016) noted that a fault that

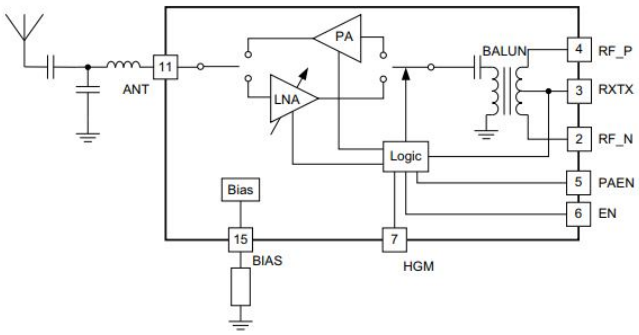

Figure 2. CC2591 Eletric Diagram (Instruments, 2014).

cause link asymmetry may influence the communication between two neighbors. Figure 3 shows an usual hardware architecture for transceivers with external PA.

It is noticed that the signal reception (RX path) is different from the path to the transmission (TX path), which passes through a PA. For this reason, a PA fault does not compromises the sensitivity of receiving signals, but rather the transmission. Note that this fault is different from a signal block, in which there is symmetry (loss of power transmitted and received).

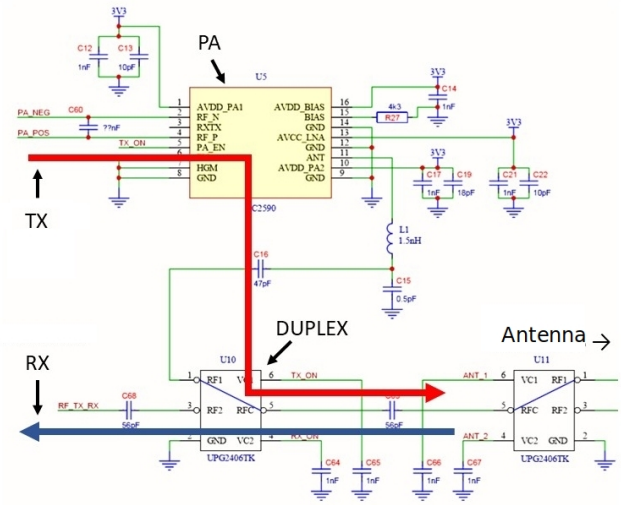

Figure 3. Usual transceiver hardware architecture (Krötz, 2019).

Thus, it is clear that a problem in PA can lead to asymmetric communication. In other words, the radio with PA fault is able to receive the messages from its neighbors. However, depending on the distance, they might not listen to the radio that has the fault. This can seriously influences IWN communications. In this case, as mentioned previously, healthy radios may not receive NM messages, giving the impression that they are having problems, when in fact the problem is in the intermediate radio

4. METHOD FOR LINK FAILURE DETECTION

The detection of the exposed problem is fundamental to maintain the network in proper operation. Detecting this kind of fault sometimes is a complex task. Erroneous

diagnosis can lead to wrong conclusions about a particular network failure. One of the cases, which is the problem presented in the Subsection 3.4, was detected in laboratory work.

The tool developed in Krötz (2019) allows to evaluate latency and edit topologies in WH networks. In addition, the tool is also able to insert faults in the network. One of these failures is to disable the PA of a device. The tool allows to apply the methodology proposed in the IWN.

Figure 4 shows the flowchart of the network failure monitoring method. The algorithm compares RSL values at different times throughout network operation. The RSL values are stored in matrices at each algorithm iteration. These matrices store information obtained through command 780.

Command 780 is initially sent to all devices on the network. If it is first a request, the RSL values of the neighbors of each device are stored in the m_1 two-dimensional array. If it is the second request, the values are stored in the m_2 two-dimensional array. A comparison between the two matrices is performed in order to verify whether there are significant differences between the RSL of the matrix m_1 and the matrix m_2. If there are differences, an indication will occur. At each iteration the matrix m_1 is updated with the values of the matrix m_2.

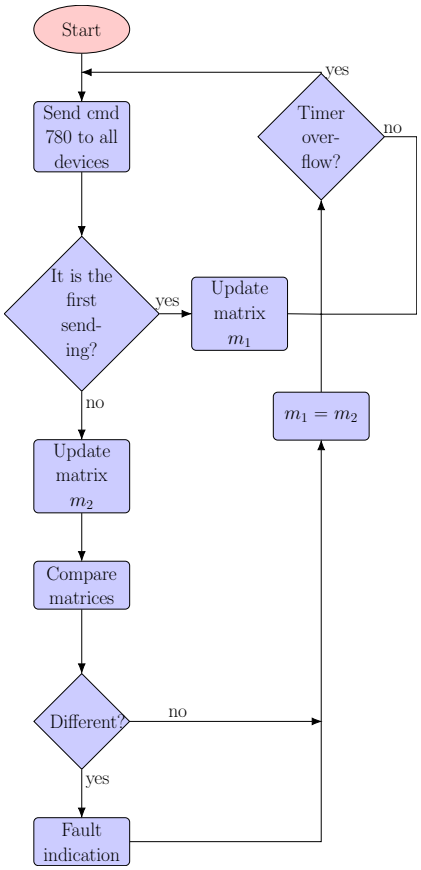

Figure 4. Link failure detection algorithm flowchart.

After the new data (matrix m_2) is stored a timer is started and finished after 10 minutes. This period was adopted because the command 780 is based on an average value of RSL, according to the Subsection 3.2. This prevents the value of RSL from being too close to the value of the first acquisition.

The rows and columns of the matrices are composed by command 780 informations, as mentioned in Section 3.1. The Figure 5 shows that the first column refers to the nickname of the device to which the command was sent. The position $2 * n + 1$ indicate to the neighbor's nickname and position $2 * n + 2$ to the respective RSL that is perceived. The n indicator represents the number of neighbors the device has. During the execution of the algorithm the command 780 is sent to all devices on the network. In this way each matrix's row refers to one field device, their respective neighbors and the RSL of communications.

NICK_0	NICK_viz0	RSL_0	NICK_viz1	RSL_1	NICK_viz2	RSL_2	...
$A_{0,0}$	$A_{0,1}$	$A_{0,2}$	$A_{0,3}$	$A_{0,4}$	$A_{0,5}$	$A_{0,6}$	$A_{0,j}$

NICK_1	NICK_viz0	RSL_0	NICK_viz1	RSL_1	NICK_viz2	RSL_2	...
$A_{1,0}$	$A_{1,1}$	$A_{1,2}$	$A_{1,3}$	$A_{1,4}$	$A_{1,5}$	$A_{1,6}$	$A_{1,j}$

Figure 5. Matrices of command 780 data.

For the execution and validation of the proposed algorithm, experiments were performed and the steps are described below.

4.1 Creating the Topology

Initially, three devices are connected to the network. The devices connect to the gateway through the NAP. Figure 6 shows the connections between devices. Lines with two arrow ends illustrate that there is communication in both directions (reception and transmission). Case some line only shows one arrow, it means that the communication is not bidirectional. In this topology, it is noticed that the distance between FD2 and FD3 is considerably smaller than the distance FD4 is from FD2, which can occur in an industrial application. It is important to note that the FD4 device does not have a direct link to the NAP, that is, packets generated in FD4 must pass through FD2 to get to the NAP.

The algorithm responsible for monitoring the RSL values is executed in a host application. The algorithm is executed periodically and performs the comparison of the current RSL values with the previous ones.

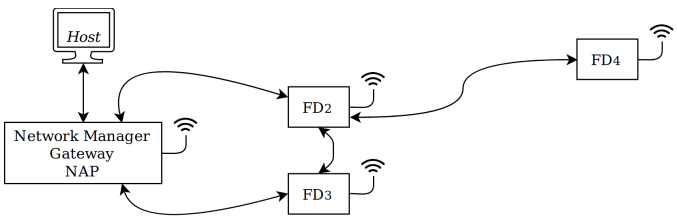

Figure 6. Network setup to proposed method validation.

4.2 Failure Insertion

In this step an artificial fault is inserted in one of the devices using the tool developed in Krötz (2019). A command is sent to one of the devices to disable the PA. The effect of this command emulates a PA fault. PA malfunctions result

in loss of transmission power, however does not impact the reception of messages by the the device. Considering that FD2 had its PA disabled to transmission, FD4 stop to listen FD2 due to the signal transmitted by FD2 has a lower level than the sensitivity of FD4. The communication between FD2 and FD3 also is impaired, but FD3 continue to listen FD2. This happens because as mentioned, FD3 and FD2 are close to each other and FD4 is not.

The Figure 7 shows the topology after the failure insertion. It is noticed that the transmission link from FD2 to FD4 is not more represented (unidirectional edge between FD2 and FD4), since as mentioned FD2 transmission is not happening properly.

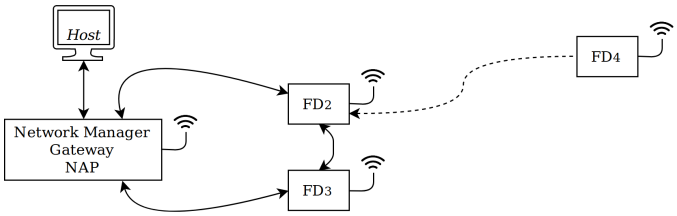

Figure 7. Device FD2 with PA failure.

4.3 Statistical Analysis

To determine the level of signal degradation that represents a PA failure, a statistical analysis was performed. The analysis is based on 10 samples of experiments. Each sample is obtained by the difference in RSL from the neighboring device to the device affected by the failure. This difference will be calculated using the data from matrix m_1 (pre-failure) and m_2 (faults). Due to the number of samples collected, Student's t-distribution was used.

The graph of the Figure 8 presents 10 samples of tests analyzed, which include the pre and post failure RSL values.

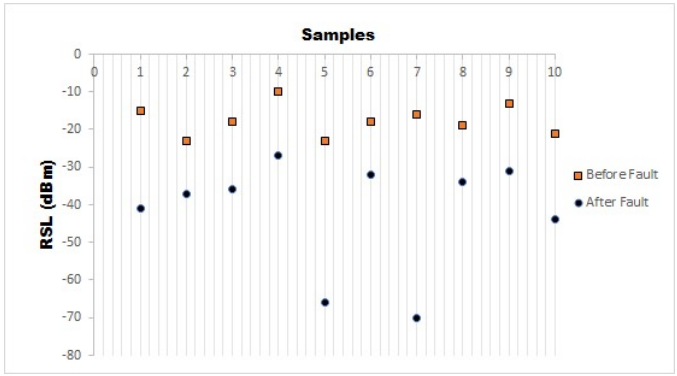

Figure 8. RSL levels before and after failure.

Below, the calculated values of the mean (in absolute) of the levels of pre and post failure RSL, the standard deviation and variance is shown below.

The mean differences in RSL levels were used as a simple matter: even though the network setup is exactly the same, i.e. radios and access point are in the same position, there are other factors inherent to the IWN that influence tests. Interference from other networks such as IEEE 802.11 and obstacles are some of these factors. It is possible to see that the gap represents something close to 25 dBm.

To find the value that best characterizes the fault and that will be used as standard at the time of the comparison between the first and second RSL evaluation, the confidence interval was calculated. With a significance level of 0.05, 10 samples and with the standard deviation already calculated, the confidence interval calculated is 9.73 dBm. This means that the difference between RSL that are within the confidence interval of 24.2 $\pm$ 9.73 dBm has 95% chance of having trouble in PA. Therefore, the default value of the difference between the measured RSL levels, which will be adopted, is 14.46 dBm, since values above the other interval 33.94 dBm there is a greater chance that a hardware problem happened. After the establishment of this confidence interval, tests were performed and are presented in the next section.

5. RESULTS

For the implementation of the link failure detection method were performed experiments following the methodology presented in the 4 section.

The topology of the experiment is presented in Figure 9, with two FDs next to each other and a distant third of them. The results were obtained by tool developed in Krötz (2019) where the collected data were stored and presented below.

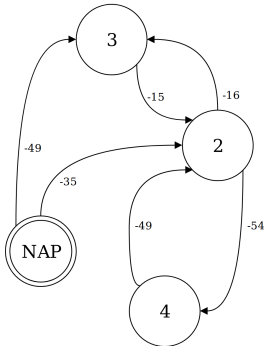

Figure 9. Network topology before PA failure.

Table 1 displays the RSL values of the neighbors of the devices before the fault is inserted.

Devices \ Neighbors	NAP	2	3	4
2	-35	-	-15	-49
3	-49	-16	-	-
4	-	-54	-	-

Table 1. RSL values before PA failure in dBm.

The radios that are positioned next to each other have nicknames 2 and 3. The arrows indicate RSL perceived by the device relative to its neighbor, for example: device 4 senses an RSL level of -54 dBm from neighbor 2. After insertion of the fault in the system, in which the PA of device 2 was disabled, the resulting topology is shown in Figure 10.

Table 2 displays the RSL values of the neighbors of the devices after the PA fault.

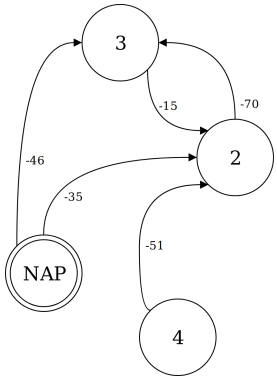

Figure 10. Network topology after PA failure.

Devices \ Neighbors	NAP	2	3	4
2	-35	-	-15	-51
3	-46	-70	-	-
4	-	-	-	-

Table 2. RSL values after PA failure in dBm.

It is noted that upon insertion of the failure the device 4 is not able to receive the transmissions of the device 2. In addition, the RSL that the other devices perceived from device 2, dropped significantly. Comparing with the network before fault, present in Figure 9, it is notice that the device 3 received from 2 with an average power of -16 dBm. After the fault insertion, the average value dropped to -70 dBm.

As previously discussed, the loss of a link between devices 2 and 4 may to cause the NM to understand that device 4 is outside the network. If this may occur, device 4 may be replaced in order to attempt to correct the problem. Clearly the wrong diagnosis of the network led to a wrong and inefficient solution to the problem. Nevertheless, the algorithm detects that there has been a significant loss of power on the transmissions of the device 2 and informe the user that the radio is not working correctly. In this way, it is possible to obtain a correct diagnosis of the network thus preventing healthy devices like device 4, to be replaced at the same time that a failed device like device 2 is kept in the network.

Due to the characteristic of the WH networks, where the topology is usually in a mesh, the packets have reducing paths to reach the destination. Therefore, even if a failure occurs in a device PA, it may be that none device is disconnected from the network. For example, if FD4 had a connection to FD3, it would probably continue to be part of the network. Nevertheless, this type of problem can lead to an increase in the loss of packets and consequently the reduction of network reliability. The algorithm presented in this work is able to detect this type of problem independently of the disconnection of a device, since the RSL of all links in the network are evaluated.

6. CONCLUSIONS

The IWN present a number of challenges for researchers and developers, as the harsh environment that is often faced in industrial environments. A important point is to have of good network evaluation tools, which can verify the parameters of performance. At some moments, where there are no information about failure, wrong decisions can be made by maintenance technician.

This work presented a method to analyze transmissions in IWN, being able to validate such method in a controlled environment with a known topology. The case study described has brought a topology with 3 field devices, which only one would have its hardware affected through a fault simulation in its PA. The failure hampered transmission of packets with the farthest device, but the field device maintained sufficient power to communicate with its nearest neighbors. This failure caused the farther radio to lose its connection to the network, leading to an erroneous interpretation. The method proposed in this work was able to present the true diagnosis, ascertained through the RSL levels of the network radios, in fact pointing out the problem device.

A statistical analysis was performed in order to find the reliability of the transmission attenuation between pre and post failure RSL levels. Through the analysis it was determined that the radio having an attenuation of 24.2± 9.73 dBm has 95% chance of the PA to be defective.

For future work it is suggested to study the behavior of the network by inserting failure on more than one device at a time. In addition, failures beyond hardware could be applied. A point to be verified later and serves as a reference, which the algorithm does not contemplate, is the fact that there is the insertion of a DF already with a failure in the AP. If this happens, the algorithm will not detect it, as there is no previous history of operation for comparison. An example would be the use of physical objects between the devices, affecting the levels of RSL thus placing the confidence interval calculated for the analyzed topology. Another suggestion, would be to establish a correlation with the lost packet rate, even more reliable to the method.

REFERENCES

Chen, D., Nixon, M., and Mok, A. (2010). *WirelessHART^{TM}: Real-time mesh network for industrial automation*. Springer, New York.

Foundation, H.C. (2007). HCF_SPEC-065, Revision 1.0 2.4GHz DSSS O-QPSK Physical Layer Specification.

Foundation, H.C. (2008a). HCF_SPEC-075, Revision 1.1 TDMA Data Link Layer Specification.

Foundation, H.C. (2008b). HCF_SPEC-155, Revision 1.1 Wireless Command Specification.

Instruments, T. (2014). *CC2591 2.4-GHz RF Front End*.

Kenyeres, J., Kenyeres, M., and Rupp, M. (2011). Experimental Node Failure Analysis in WSNs. *18th International Conference on Systems, Signals and Image Processing (IWSSIP)*, 1–5.

Krötz, C.A. (2019). *Ferramenta e Método Para Obtenção de Parâmetros de Confiabilidade Fim-a-fim de Redes Industriais Sem Fio*. mastersthesis, Universidade Federal do Rio Grande do Sul.

Kunzel, G., Winter, J.M., Muller, I., Pereira, C.E., and Netto, J.C. (2012). Passive monitoring software tool for evaluation of deployed WirelessHART networks. *Brazilian Symposium on Computing System Engineering, SBESC*, 7–12.

Machado, T., Muller, I., Winter, J., Dickow, V., Pereira, C.E., and Netto, J.C. (2014). WirelessHART network analyzer with coexistence detection. *Proceedings - 2014 12th IEEE International Conference on Industrial Informatics, INDIN 2014*, 696–701.

Machado, T.M., Muller, I., Winter, J.M., Dickow, V.H., Netto, J.C., and Pereira, C.E. (2013). Ferramentas para inspeção e análise de redes wirelesshart: comparação e avaliação dos métodos existentes e proposta de uma nova ferramenta. *Safecomp 2013 FastAbstract*, 1, 1–6.

Maheswar, R. and Jayaparvathy, R. (2012). Performance analysis of fault tolerant node in wireless sensor network. In V.V. Das and J. Stephen (eds.), *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering*, volume 108 LNICST, 121–126. Springer Berlin Heidelberg.

Muller, I., Pereira, C.E., Netto, J.C., Fabris, E.E., and Allgayer, R. (2010). Development of a WirelessHART compatible field device. *2010 IEEE International Instrumentation and Measurement Technology Conference, I2MTC 2010 - Proceedings*, 1430–1434.

Müller, I., Winter, J.M., De Freitas, E.P., Netto, J.C., and Pereira, C.E. (2012). Towards WirelessHART protocol decentralization: A proposal overview. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, volume 7469 LNCS, 248–259.

Nobre, M., Silva, I., and Guedes, L.A. (2014). Reliability evaluation of wirelesshart under faulty link scenarios. *Proceedings - 2014 12th IEEE International Conference on Industrial Informatics, INDIN 2014*, 676–682.

Silva, I., Guedes, L.A., Portugal, P., and Vasques, F. (2013). Common Cause Failure Analysis for Wireless Sensor Networks. *Safecomp 2013 FastAbstract*.

Virkki, J., Zhu, Y., Meng, Y., and Chen, L. (2011). Reliability of WSN Hardware. *International Journal of Embedded Systems and Applications (IJESA)*, 1(2), 139–10.

Wang, Q. and Jiang, J. (2016). Comparative examination on architecture and protocol of industrial wireless sensor network standards. *IEEE Communications Surveys and Tutorials*, 18(3), 2197–2219.

Wang, Y., Xing, L., and Mandava, L. (2018). Probabilistic competing failure analysis in multi-state wireless sensor networks. *Proceedings - Annual Reliability and Maintainability Symposium*, 2018-Janua, 1–7.

Winter, J.M., Pereira, C.E., Netto, J.C., Souza, F.A., Muller, I., and Catunda, S.Y. (2016). Analysis of a radio physical layer fault in WirelessHART networks. *Conference Record - IEEE Instrumentation and Measurement Technology Conference*, 2016-July, 1–5.