Avoiding down times – Monitoring, diagnostics and troubleshooting of industrial wireless systems

Andreas Frotzscher and Ulf Wetzker
Fraunhofer Institute for Integrated Circuits IIS, Division Engineering of Adaptive Systems EAS, Dresden, Germany
{*andreas.frotzscher, ulf.wetzker*}*@eas.iis.fraunhofer.de*

***Abstract*—The ever-growing proliferation of wireless devices and technologies used for Internet of Things (IoT) applications, such as patient monitoring, military surveillance, and industrial automation and control, has created an increasing need for methods and tools for connectivity prediction, information flow monitoring, and failure analysis to increase the dependability of the wireless network. Indeed, in a safety-critical Industrial IoT (IIoT) setting, such as a smart factory, harsh signal propagation conditions combined with interference from coexisting radio technologies operating in the same frequency band may lead to poor network performance or even application failures despite precautionary measures. Analyzing and troubleshooting such failures on a large scale is often difficult and time-consuming. In this paper, we share our experience in troubleshooting coexistence problems in operational IIoT networks, pointing out the need for a userfriendly, automated failure analysis system. Furthermore we present a new solution addressing this demand, developed for mobile and the permanent monitoring and troubleshooting scenarios.**

I. Introduction

In industrial automation, wireless communication systems offer several key advantages over wired solutions, e.g. greater flexibility, low installation costs, great opportunities for future retrofits and extensions. Nowadays wireless communication systems are employed in industrial automation applications for instance for connecting movable machine parts, mobile subsystems, human machine interfaces or assembly tools. The global trends of the Industrial Internet of Things (IIoT) and smart factory will accelerate the market penetration of industrial wireless communication systems. According to MarketsandMarkets, wireless will at least grow to a share more than 10% of the global industrial communication market in 2022 [1]. This makes the wireless part a 15 Billion US$ market in 2022.

Due to cost reasons and market acceptance, component providers of industrial wireless communication systems in the factory automation use typically existing wireless technologies, operating in the license-free frequency bands, e.g. WiFi (IEEE 802.11), Bluetooth, Bluetooth Smart, Bluetooth Low Energy (BLE), IEEE 802.15.4 (the basis for several low-rate wireless personal area and industrial networks such as ZigBee, ISA100.11a, and WirelessHART) and radio frequency identification (RFID) systems. In the future a set of other emerging technologies and solutions will appear in these frequency band, e.g. Long-Term Evolution in unlicensed spectrum (LTE-U, LTE-LAA and MuLTEfire).

Despite of its simplicity, wireless communication systems employed in industrial applications pose several problems to the user. First, most of the wireless technologies currently in use are not design for industrial applications, where guaranteeing high packet reception rates, bounds on end-to-end packet latency, and continuous system availability are of utmost importance [2], [3]. Second, these technologies use overlapping frequencies, resulting in interference from neighboring devices, indicated by packet losses, unpredictable medium access delays, and high end-to-end latencies. Third, these technologies do not contain sufficient self-monitoring and diagnostic functionalities.

Our experience in troubleshooting coexistence problems in operational Industrial Internet of Things (IIoT) installations shows that this is often a labor-intensive and time-consuming task. The main reasons for this are that the process is largely manual, involves the use of many different tools, and requires expert knowledge in diverse fields. Many companies can not afford such experts and depend on specialized troubleshooting service providers, causing additional delay during the troubleshooting. As most of the wireless connectivity problems occur sporadically, a proactive monitoring and diagnostic of the wireless communication system is necessary. However, existing troubleshooting tools are not suited for this, nor are they capable to diagnose failures in heterogeneous wireless infrastructures in depth or to provide hints on how to fix them [4]. This is a major hurdle for engineers debugging cyber-physical and IIoT systems deployed on a large scale in remote locations. This lack of tools makes troubleshooting industrial wireless networks an exasperating, labor-intensive, and time-consuming task – sometimes a real *agony*.

This paper presents a new monitoring and diagnostic solution for industrial wireless networks. It analyzes the spectrum of the considered frequency band and the logical data of the wireless telegrams and by this, allows an automatic in depth analysis for on-sight troubleshooting and an off-line examination in case of more complex problems.

The paper is structured as follows. In Sec. II we share our experiences from customers and operators of IIoT systems, giving an overview of typical problems users of industrial wireless applications are faced to nowadays. In Section III first the requirements on a monitoring and troubleshooting system are summarized briefly and then our new solution is presented. Section IV concludes this paper.

II. Typical problems in current industrial wireless applications

Nowadays, during the commissioning of a new wireless communication system for industrial applications first a frequency planning will be done to avoid coexistence problems with neighboring wireless networks. Second a site survey is conducted, to measure the receive power of the wireless access points, gateways or master nodes at a collection of important positions. Sometimes also throughput measurements are conducted as well.

However, even when following best-practice principles with precise connectivity information [5], it is hard to predict how the environment changes over time and therefore very difficult to ensure correct operation on a large scale for prolonged periods of time, even for technology experts. The propagation conditions of the wireless signals will vary over time, e.g. due to moving objects, new machinery equipment or reconstructions at the shop floor. This results in a time varying coverage and might cause outage and connectivity loss in some areas.

Although considering the coexistence to other wireless networks during the commissioning phase, other wireless devices may appear at a later time and can cause inter-network-interference. This can be rogue access points setup temporarily by subcontractors or even cell phones. These rogue devices might interfere the industrial wireless communication systems and can provoke down times of the industrial applications. In order to give an example, in one real world scenario the cell phone of an employee caused sporadic failures of an production cell in an automotive factory. The failures had a noticeable correlation with daytime. Nevertheless the maintenance staff could identify the failure root cause only after three weeks of intense analysis.

In large wireless infrastructures, e.g. for connecting automated guided vehicles in intralogistics applications, wireless clients suffer from connection losses due to failures during the roaming procedure between access points.

Another failure source is the misconfiguration of the wireless equipment with respect to the requirements of the application. In another real-work scenario an IO device on a rotating platform were connected to the controller using WiFi. At a later stage more IO devices were mounted on the platform and connected via WiFi. Afterward the controller suffered from repeated failures, as the wireless communication system could not reliably handle the increased traffic at the same timing constraints.

In practice, also simple hardware defects occur regularly, such as broken antenna cables, damaged or broken antennas. In outdoor areas we even found antennas with water inleakage. The variation and degradation of the wireless devices itself are additional typical failure sources.

Troubleshooting the problems discussed above is mostly very difficult due to several reasons. First, in most cases connectivity problem are detected not before the application exhibits failures. Second, the evidence of most of the discussed failure sources appear sporadically. Third, a large variety of root causes can provoke application failures. Besides the wireless communication system, the wired communication infrastructure, the IT systems and software (e.g. firewalls, data bases, management systems) are further sources of failures.

III. Monitoring, Diagnostics and Troubleshooting of industrial wireless networks

Industrial wireless networks need to be monitored and analyzed during the complete life cycle. Specifically, the following use cases can be identified:

1) installation,
2) commissioning,
3) inspection and
4) troubleshooting.

A. Requirements

Since the target users are mainly maintenance staff and system integrators the following five requirements are set on monitoring and troubleshooting systems for industrial wireless networks.

1) **Automated:** The failure analysis should be automated by implementing a black box approach without requiring manual interventions to speed up the troubleshooting process.
2) **Interactive:** Online processing and concurrent analysis algorithms are needed to allow for an interactive observation of the continuous data stream from all monitoring devices.
3) **Comprehensive:** The system should detect all wireless standards and technologies using the considered frequency band. Cross-technology observations and analysis should be performed on multiple network layers.
4) **User-friendly:** To allow the use by non-experts, the system should be easy to set up and configure, and should present the results of the analysis in an intuitive and comprehensible way.
5) **Flexible:** New standards and technologies appear frequently. Thus, a flexible and extensible hardware and software design based on a generic multi-stage analysis structure is essential. Additionally, the system should support a single-node and a multi-node (*i.e.*, distributed) setup.

B. Developed failure analysis system for IIoT networks

The basic idea of the developed failure analysis system is depicted in Fig. 1. For analyizing co-located wireless communication systems in unlicensed frequency bands, the information of multiple sources need to be combined, e.g.

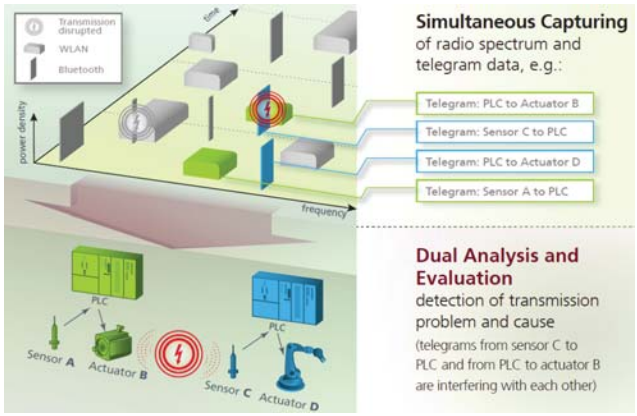

Figure 1. Concept of the developed failure analysis system for IIoT networks

spectral data, network traffic of multiple wireless standards, time and position information. By extracting the relevant meta information, the state and reliability of each individual wireless link can be estimated and the root cause of connectivity problems can be identified, e.g. interference between neighboring wireless networks. To process this extensive amount of data on systems with limited memory and processing resources, we have implemented a multistage stream based information processing system. The first two layers consists of the following main blocks: First, the analysis of the spectrogram and extraction of the relevant meta data. Second, it contains the capture of the communication standard-specific data traffic and preprocessing modules including an early data reduction, time synchronization as well as blocks to create uniform and tidy data structures. By processing the cleaned up data each subsequent failure analysis layer amplifies the degree of abstraction up to a direct indication for the original failure root cause. By this the health state of each individual wireless connection can be be analyzed and the root cause of connectivity problems caused by pathloss, intra-network interference (between nodes of the same network) or inter-network interference can be identified.

The underlying software framework is tailored towards a high performance of the analysis architecture. In addition to the block based software structure we introduced a flexible local or networked interconnection system. That way it is possible to use the developed failure analysis software framework to setup a distributed failure analysis system, where multiple monitoring and computation nodes collaborate within one analysis task. The interface towards the interconnection systems is available in different programming languages to simplify the development of highly optimized information filters as well as the prototyping of abstract algorithms.

The flexible networked interconnection system used in the failure analysis software architecture makes it possible to

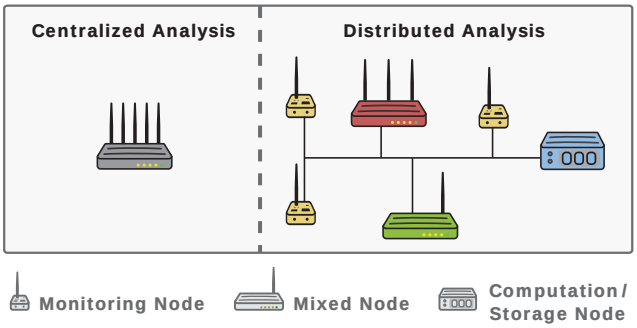

Figure 2. Centralized or distributed setup of the failure analysis system

easily integrate the failure analysis to a single monitoring node or to spead it over multiple distributed monitoring nodes. The latter allows the presence of multiple monitoring and computing/storage nodes that collaborate within one analysis task, as shown in 2. By this the different use cases explained above can be addressed cost efficiently.

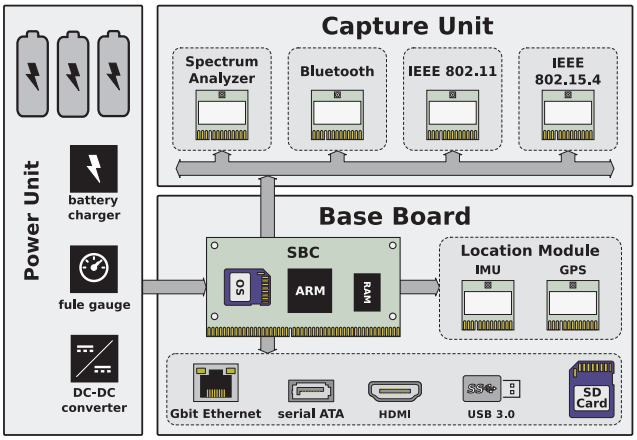

Figure 3. Overview of the proposed modular hardware platform

Because of the variety of wireless standards and the rapid development of new communication systems the hardware must be expandable and adaptable for special scenarios. Therefore, we designed a modular, robust and flexible hardware platform for the monitoring node (Fig. 3) customized towards the operation in industrial environments. The modular concept is based on affordable standard components and supports multiple transceiver modules. The functional interaction between the modular software and hardware structure of the monitoring node enables the implementation of mobile battery powered failure analysis instruments as well as permanent observation systems. This concept allows also the remote operation of the failure analysis system, enabling even new business cases for wireless network troubleshooting service providers. Figure 4 shows our developed prototyp of the monitoring node.

Figure 4. Prototype of the Wireless Network Monitoring node of Fraunhofer IIS/EAS as tool for permanent monitoring and diagnostic of industrial wireless networks

In parallel we integrated our failure analysis system also in a tablet device, the Wireless Network Analyzer. It supports system integrators and maintanence staff in mobile scenarios during the commissioning, inspection and troubleshooting. Due to the limited hardware flexibility and extendablity of the tablet solution only a single transceiver module can be used for the failure analysis, supported by an external spectral capturing module. Thus, this solution is more suited for the in-deep analysis of a single wireless technlology and the detection of network intrinsic failure causes or interference problems with other co-located wireless systems. Figure 5 shows our Wireless Network Analyzer used in practice.

Figure 5. Wireless Network Analyzer of Fraunhofer IIS/EAS as portable monitoring and diagnostic tool for industrial wireless networks

IV. Conclusions and Future Work

Troubleshooting a failure is an almost unavoidable task during the lifetime of a real-world wireless network. Inter-network interference caused by the increasing number of wireless technologies and devices within the unlicensed frequency bands increases the complexity of this task, making it difficult to identify and eliminate failures, especially in safety-critical environments.

In this paper, we have shared our experiences from customers and operators of industrial wireless networks. We presented a new solutions enabling a systematic, automated monitoring and diagnosis of wireless coexistence problems in the IIoT. One of the key features of the proposed system is its ability to simplify the observation of heterogeneous wireless communication standards and unknown sources of radio interference in the surroundings. It helps to improve the user experience and thus, accelerates the market penetration of wireless solutions in the industry.

Acknowledgments. This work was supported by the project "fast automation" and the Federal Ministry of Education and Research of the Federal Republic of Germany (BMBF) within the initiative "Region Zwanzig20" under project number 03ZZ0510A.

References

[1] *Industrial Communication Market - Global Forcast to 2022*, MarketsAndMarkets, 2016. [Online]. Available: http://www.marketsandmarkets.com/Market-Reports/industrial-communication-market-146536397.html

[2] P. Suriyachai, J. Brown, and U. Roedig, "time-critical data delivery in wireless sensor networks," in *6th IEEE Int. Conf. on Distributed Computing in Sensor Systems (DOSS)*, 2010.

[3] A. Frotzscher, U. Wetzker, M. Bauer, M. Rentschler, M. Beyer, S. Elspass, and H. Klessig, "Requirements and current solutions of wireless communication in industrial automation," in *Proc. of the IEEE Int. Conf. on Communications Workshops (ICC)*, 2014.

[4] G. Koepke, W. Young, J. Ladbury, and J. Coder, "Complexities of testing interference and coexistence of wireless systems in critical infrastructures," National Institute of Standards and Technology (NIST), Tech. Rep., 2015.

[5] ZVEI Automation - German Electrical and Electronic Manufacturer's Association, "Coexistence of Wireless Systems in Automation Technology," 2009.