Volume 124, Article No. 124007 (2019) https://doi.org/10.6028/jres.124.007
Journal of Research of National Institute of Standards and Technology

A Black-Box Noninvasive Characterization Method for Industrial Wireless Networks

Mohamed Kashef, Richard Candell, and Kang Lee

National Institute of Standards and Technology,
Gaithersburg, MD 20899, USA

mohamed.kashef@nist.gov
richard.candell@nist.gov
kang.lee@nist.gov

Industrial control systems are increasingly using wireless communications to improve monitoring and control of industrial processes. In existing installations, distances and costs for installation often prohibit the running of new cables and conduits, making wireless solutions very attractive. With costs reduced, monitoring of the physical process becomes easier, and operators often desire to extend wireless to include supervisory and feedback control. Feedback control, in particular, requires certain reliability, latency, and performance guarantees that are difficult to characterize. Industrial wireless solutions rarely make quality-of-service measurements available at the control system level. When they do, indicators such as per-link packet success rate are often difficult to translate into meaningful metrics useful to the control system designer. This is especially true for multihop mesh network architectures, where it is difficult to translate link performance to system performance. In this paper, we propose a more useful method to characterize true network latency and reliability of a deployed industrial wireless network without the need for physical layer and link layer performance metrics and design knowledge.

Key words: industrial wireless; manufacturing; networked control; process control.

Accepted: February 28, 2019

Published: March 18, 2019

https://doi.org/10.6028/jres.124.007

1. Introduction

1.1 Wireless in Manufacturing

Manufacturing processes are industrial processes that convert raw materials, components, or parts into finished goods based on engineering specifications. Categories of manufacturing processes include discrete systems and continuous systems. Discrete systems resemble automotive and aerospace vehicle production, in which parts are machined and assembled according to precision specifications, usually made economical with robotic machinery, proximity sensors, switches, and actuators. Continuous processes resemble those found in oil and gas, municipal water, and chemical production, made possible through large and often unstable thermodynamic processes. In both discrete and continuous manufacturing processes, economical and practical gains are made by either monitoring those systems through the use of sensors or control of the those systems with actuators [1]. Wherever wired solutions are possible, those sensors and actuators are interconnected using wired networking solutions; however, not all networked solutions are practical or economical. Wired solutions require expensive cables, conduits, and labor to install, making wired solutions costly, and environmental conditions can make installation of cables impractical. Hence, wireless solutions

How to cite this article:
Kashef M, Candell R, Lee K (2019) A Black-Box Noninvasive Characterization Method for Industrial Wireless Networks. *J Res Natl Inst Stan* 124:124007. https://doi.org/10.6028/jres.124.007.

may be advantageous to manufacturing operations [2]. In both discrete and continuous manufacturing systems, wireless provides the ability to sense variables of the manufacturing process and environment, and optimize, supervise, and react to change while improving safety and security of people and equipment.

1.2 Importance of System Testing

Wireless communications help to alleviate cost and flexibility constraints by being low-cost and by enabling mobility [2]. However, the industrial wireless environment can be harsh, because the surroundings are typically highly metallic, thereby creating multipath effects and severe path loss. Industrial control systems are often intolerant of communication faults and network latency, and they often require very high transmission reliability [3]. Depending on the purpose of the wireless network (monitoring, supervisory control, feedback control, or safety monitoring), understanding the system performance of the network may be critical. For feedback control systems and safety monitoring systems, understanding the performance of the network from the perspective of the industrial controller or safety alarm system is essential. However, factory operators, system integrators, and control systems designers are rarely experts in wireless communications systems. Considerations such as electromagnetic propagation, antenna efficiency, path loss exponents, packet error rates, and medium access are often foreign concepts to factory engineers. Even if factory engineers were expert in wireless theory and design practice, the information that they would need to make educated decisions is usually unavailable. When available, link quality metrics such as packet loss ratios are informative but can be difficult to understand with complex mesh architectures and routing algorithms. Moreover, it is generally difficult to measure these quantities for operational networks. The control system design will only need to know the statistical distribution of latency and reliability of information transmission through the network to design a controller that is robust. Therefore, a practical method for characterizing the performance of the wireless network that does not require an in-depth understanding of wireless communications or electromagnetic wave propagation is needed.

The primary objective of the test method proposed here is to evaluate the performance of a wireless network deployed in an industrial environment. It is assumed that detailed metrics of the network operation such as physical and medium access control (MAC) layer performance metrics are not available. Hence, the node placement and transmission parameters effects can be easily characterized to decide the usefulness of adding or positioning a node in a wireless network.

1.3 Related Work

The problem of studying the performance of industrial wireless networks has been studied from different perspectives in previous research. First, simulations of industrial wireless networks have been conducted to study various performance measures, such as in Refs. [2, 4–7]. Second, the performance has been measured using hardware experiments, such as in Refs. [8–15].

In the simulation-based performance analyses, the packet-level measures are easily monitored throughout the simulation. In Ref. [2], a simulation framework was introduced for using a WirelessHART communication network in a process control system where all packet-level parameters are controlled and monitored. The performance is evaluated by studying the effect of various parameters, including cost, production rate, and the flow rates of various process components. In Refs. [4, 5], the use of various simulation packages for simulating wireless networks in cyberphysical systems was considered. Moreover, in Ref. [6], an ISA100.11a system was studied, where the effects of the time slot duration, superframe period, and back-off exponent on various packet-level measures such as throughput, average delay, and energy consumption were evaluated. Finally, in Ref. [7], the reliability of an industrial wireless network was studied through measuring the communication latency and stability at the packet level.

On the other hand, hardware-based analyzing or testing tools, such as that in Ref. [8], have been used to monitor packet-level measurements while studying network performance for compatible hardware experiments. Also, generic or laboratory built wireless nodes can be used to allow monitoring of packet flows in wireless networking scenarios. In Refs. [9, 10], a wireless network, which been developed by the authors, was used to monitor a turbine power generation system, where various performance metrics could be directly measured within the wireless network. In Refs. [11, 12], Institute of Electrical and Electronics Engineers (IEEE) 802.15.4a development boards were used as the network devices, where configuration and monitoring could be easily done through an attached computer. Similarly, in Ref. [13], single-hop transmissions using Wireless Networks for Industrial Automation - Process Automation (WIA-PA) protocol were evaluated using accessible hardware where packets are controlled. Also, in Ref. [14], wireless stations that are compliant with both IEEE802.11g and IEEE802.11e specifications were used for wireless communications where response time was measured in a four-node network. Finally, in Ref. [15], Zigbee programmable nodes were used for industrial communications where the performance could be measured directly.

Similarly, in Ref. [16], the quality of wireless service in a factory floor was evaluated by measuring the received signal strength (RSS) of the transmitted signals. The goal in that work was building a tool to optimize the wireless coverage, where radio frequency measurements were collected and used in the analysis. In Ref. [17], the effects of different wireless physical factors were studied, including physical position, transmission power, link direction, transmission frequency, and line-of-sight availability. An experimental study on these effects was performed over an industrial wireless network using the RSS indicator (RSSI) of the signal at various locations as the main evaluation criterion. In Ref. [18], the impact of various wireless impairments was studied through characterizing the bit and symbol error rates. The statistics were obtained through actual industrial deployment. In Ref. [19], the idea of injecting virtual signals through an industrial network was introduced, where on-board virtual sensors were added to the wireless devices to allow for this task. The goal of that work was to provide a tool for virtual sensor control and to study the memory and performance overhead on the wireless devices. In Ref. [20], the effect of interference on an industrial wireless network was studied experimentally to allow for network control to be optimized based on coexisting interference. The packet polling round-trip time and cycle time criteria were used for performance evaluation to characterize interference effects on dropping and delaying packets transmitted over the network.

In all these related works, packet-, bit-, or signal-power-level performance measurements were considered, using simulations, hardware monitoring tools, or experimentally developed networks. Testing for available wireless node performance without knowledge about internal operation, especially in industrial applications, is important. Hence, in this paper, we introduce a test method for industrial wireless networks at the signal level, including characterization of the quality of the received signal. We adopt the idea of injecting a virtual sensing signal [19] to obtain the signal-level characterization of an industrial wireless network.

1.4 Paper Organization

Our contributions in this work can be summarized as follows:

- We propose a test method to characterize industrial wireless network performance without requiring access to packet-level transmission parameters.
- We describe the use of a testbed composed of industrial wireless networking components and a channel emulator to include the effects of industrial wireless channels.

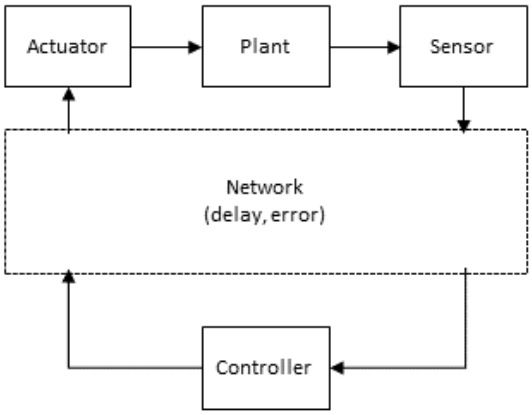

Fig. 1. A generic network model for performance characterization that consists of a digital network. The controller has direct access to digital information stored in the network.

- We assess the performance of the proposed test method using the testbed to illustrate the effectiveness of the method. Moreover, we compare various channel models to evaluate the ability of the proposed method to distinguish among various channel qualities.

The rest of the paper is organized as follows. In Sec. 2, we describe the general system model, the testbed, and the tested channel models. In Sec. 3, we detail the proposed test method. Then, in Sec. 4, we discuss the obtained experimental results and industrial network characterization. In Sec. 5, we draw conclusions. Finally, in Sec. 6, we discuss future directions of this work.

2. System Modeling

2.1 Generic Cyberphysical Model

Generic network models have been proposed, such as the one defined in Ref. [21], in which the plant is connected to the network through sensor and actuator interfaces and the controller has direct access to the information transferred within the network, as shown in Fig. 1. Such models accurately represent most industrial networks, in which the network transfers information reported by sensors, computes a control decision, and forwards that decision to the actuators. Wireless mesh networks developed using the IEEE 802.15.4 standard fall nicely within this category, assuming that actuation is supported. However, the model neglects to include the impact of signal domain conversion and assumes that the controller has direct access to sensor data transported by the network.

Some effective networking technologies used for industrial applications are designed to serve as "wire-over-wireless," in which wired industrial interface analog signals, serial data, or Ethernet data are routed over a wireless transport, making the sensors, actuators, and controller unaware of the wireless transport mechanism. In a typical wireless deployment, an industrial analog signal at 4–20 mA or 0–10 V is transmitted by a sensor or received by an actuator with a wireless transport intermediary. For these reasons, we propose the generic model for an industrial wireless network shown in Fig. 2, which includes optional analog-to-digital and digital-to-analog blocks. This extended model therefore not only includes latency and noise effects of the network, but it also includes domain conversion errors such as thermal noise, quantization noise, gain imbalances, and direct current (DC) offsets.

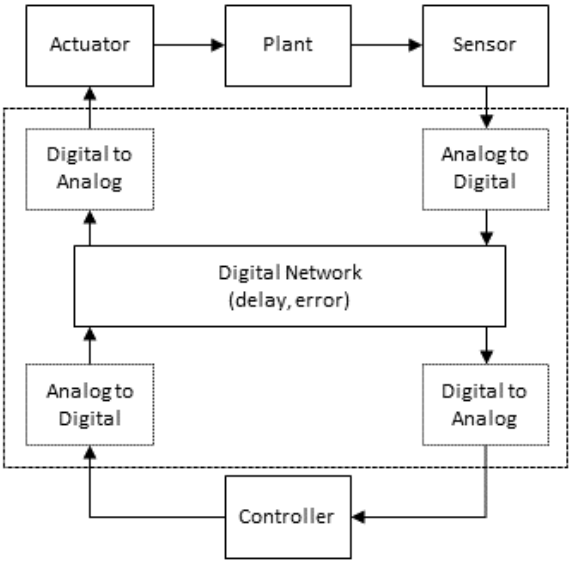

Fig. 2. An extended generic network model for performance characterization that consists of a digital network with optional domain conversions at the network boundaries. Domain conversion is an important aspect of network devices that is often overlooked.

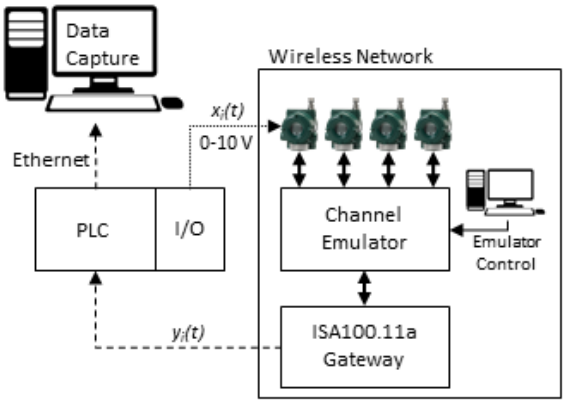

Fig. 3. The industrial wireless testbed used to validate the proposed test method using real-world network devices. In this realization, the PLC generates a data sequence that is mapped to a 0–10 *V* signal. Generic ISA100.11a devices are used to achieve wireless connectivity through a channel emulator to implement the industrial wireless environment. I/O indicates input/output.

2.2 Testbed Architecture

The proposed test method was validated using an industrial wireless continuous process testbed. The testbed is a reconfigurable platform that was designed to evaluate the effects of wireless communication technology on a continuous process such as a chemical reactor using various modes of wireless communications. A sensor-only depiction of the testbed is shown in Fig. 3. The testbed is composed of a high-performance programmable logic controller (PLC) where virtual stimuli are produced. These virtual stimuli are signals that represent typical signals in certain industrial plants. These signals may include gas

accumulations, which are realized by a charging exponential waveform, or a tank level, which is realized by a ramp waveform. The PLC is equipped with 16 bit digital-to-analog (D/A) conversion modules, which convert digital stimuli to 0–10 V analog signals, $x_i(t)$.

We denote the studied wireless network by the black box because the network specifics are not assumed to be available to the proposed test method. The wireless ("black box") network is composed of the wireless devices and infrastructure equipment. We used Ultra Electronics 3eTI iMesh industrial wireless network devices. We deployed a radio frequency channel emulator capable of replicating the multipath and path loss environment for a mesh network of up to 8 physical nodes and 56 virtual links between those nodes. The channel emulator was RFnest D508, and the corresponding software was RFview [22]. The channel emulator supports an instantaneous bandwidth of 250 MHz (4 ns tap spacing) with an effective dynamic range of 73 dB, which includes all analog and digital realization impacts. The emulator is controlled by a nearby computer, which loads the path loss model and channel impulse response for each communications link. The transmitted signal is received by a wireless gateway, which plays two roles. First, it helps in the wireless communications within the network through packet exchange for synchronization and provisioning. Second, it plays the role of the interface between the industrial controller and the wireless network by having compatible industrial protocol capabilities. The output of the wireless network is $y_i(t)$ in the figure. Since time is maintained by a single entity, the PLC, no synchronization is required for correlation of the stimuli to the outputs, $y_i(t)$. The PLC sends both signals $x_i(t)$ and $y_i(t)$ to the data-capture computer, where the delay estimation is performed.

The wireless network we use as an example is based mainly on the ISA100.11a standard. The MAC protocol of ISA100.11a employs time division multiple access (TDMA) with reserved and shared slots. A carrier sense multiple access with collision avoidance (CSMA/CA) protocol is used in the shared slots. The nodes are synchronized with time slot length between 10 and 12 ms. The schedule of time slots is generally built from a collection of time slots denoted by a superframe. The lengths of the time slots and superframe are specified by changing parameters in the transmitted packets [6]. However, the main advantage of the proposed test method is in the evaluation of the black-box end-to-end performance without knowledge of the network implementation or packet-level metrics.

2.3 Channel Models and Integration

In the testbed, we employed a channel emulator to include industrial environment effects in wireless transmissions. Generally, industrial wireless environments can be harsh, because the surroundings are typically highly reflective and resonant, thereby creating significant multipath effects. Hence, it is important to exploit the proposed test method over the industrial wireless channel. In this subsection, we briefly describe the two channel models that were considered in this work. We also describe the application of these models using the channel emulator.

First, we considered the IEEE802.15.4a channel model for industrial environments [23]. We considered models with and without a line-of-sight (LOS) component. Models without an LOS component are referred to as non-line-of-sight (NLOS). The IEEE 802.15.4a model is a generic channel model using log-distance path gain, and a modified Saleh-Valenzuela model for multipath effects. The model has been described and implemented by Molisch [23]. The values of various channel parameters were obtained using the measurements in Ref. [24]. Note that these measurements were used to fit the generic channel model.

Second, we considered a measured delay profile of an industrial environment [25] where measurements are directly processed to be converted into an example of a channel impulse response in industrial environments. Both LOS and NLOS models were considered. In both the IEEE802.15.4a and the measured channels, following the injected channel impulse responses (CIRs), the emulator produces random Rayleigh fading channels for the NLOS cases and random Rician fading channels for the LOS cases.

The two industrial channel models, with their LOS and NLOS versions, have multipath effects in their CIRs. They were compared to the benchmarks of the free space wireless model, and of the log-distance ideal models without multipath with both LOS and NLOS versions. These log-distance models have the same loss exponents as their counterpart IEEE802.15.4a and measured channel models, but they have an ideal single-tap CIR.

Finally, the channel models were applied using the channel emulator. The emulator implements a finite impulse response (FIR) filter at its core. The computational limitations of the channel emulator constrain the FIR filter to 13 taps. The produced CIR is defined using a maximum of 13 taps, where the tap spacing can take values that are multiples of 4 ns. In order to use the obtained CIR for channel emulators, we used the technique introduced in Ref. [26] to both resample and reduce the number of the taps of the CIRs within the limitations of the emulator. The N-tap CIR was obtained by fractionally resampling the original CIR to 250 MHz while maintaining the total power, the mean delay, and the root mean square (RMS) delay spread.

3. Test Method

In this section, we describe the test method proposed in this work. The primary objective of this test method is to evaluate the performance of a wireless network deployed in an industrial environment. It is assumed that network operation metrics such as physical and MAC layer performance metrics are not accessible. Thus, we propose a two-stage method for assessing the performance of an industrial wireless network using process variable (PV) signals. The method calls for estimation of network delay using maximal length pseudorandom binary sequence correlation followed by estimation of the signal error through the network adjusted by the delay estimate.

Using this method, we injected a known PV signal and monitored the PV signal at the output of the wireless network at the point where it is considered to be usable by another network node. The network is considered to be a “black-box” from edge to edge. The PV signals can represent any type of signal coming from either plant or controller, and the type of signal is irrelevant to the test method, although it is advisable that the signal conform to a standard industrial protocol. For analog signal, we recommend the typical industrial sensing and control signals of 4–20 mA or 0–10 V. For digital signals, we recommend a typical industrial communications protocol; however, the hardware used to implement the method will dictate the protocols used. Moreover, the required synchronization for delay estimation can be achieved through a temporary wired or wireless (on a different channel not to cause interference) channel to connect the input and output nodes. The architecture of the test method for various devices and signal control points is shown on Fig. 4. The proposed test method in its current form is sufficient for testing continuous process signals when packet-level statistics are not exposed. On the other hand, the packet-level metrics such as packet loss and delay are still important in the case of critical control commands.

In the following subsections, we discuss various types of input signals to be introduced for the wireless network. We discuss the analysis tools used and the performance criteria considered for characterizing a general industrial wireless network. We split the testing procedure into two stages for delay estimation and error estimation.

3.1 Delay Estimation

We exploited the conventional general cross-correlation (GCC) method for delay estimation [27]. The main advantage of this method is its simplicity compared to other delay estimation techniques. Various algorithms for calculating time of arrival (ToA) can be used. This GCC method is used when the delays are statistically stationary. Other techniques, such as the method of least mean square time-delay estimation (LMSTDE), can be used for nonstationary cases [28].

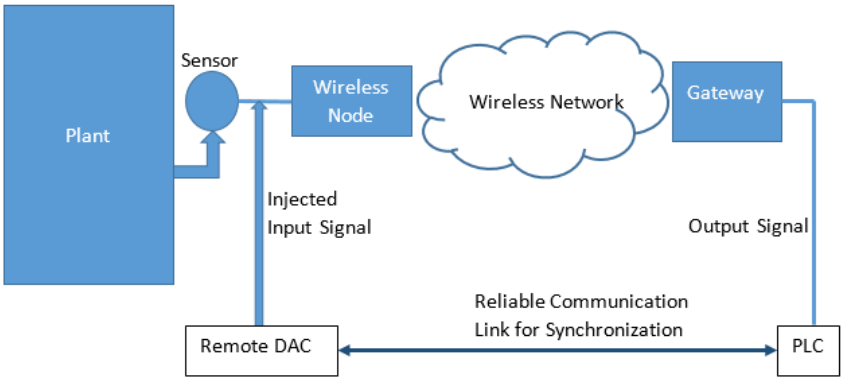

Fig. 4. The test method architecture for the case of sensor to gateway transmission. DAC indicates digital-to-analog converter.

We denote the input signal of the first stage to the tested wireless network by $x_1(t)$. This signal is an analog signal following the same characteristics of the electrical signals created by sensor nodes. The output signal is denoted by $y_1(t)$, which is a delayed and distorted version of the input signal. In order to obtain a good delay estimation using the GCC method, we choose an input signal with no repeating patterns within the window of delay estimation. Thus, we use a maximal length binary sequence generated by maximal linear feedback shift registers (LFSRs). In this work, we use an 8 bit maximal shift register with the following polynomial $P(x)$ to generate $x_1(t)$, where $P(x)$ is

$$P(x) = x^8 + x^6 + x^5 + x^4 + 1, \tag{1}$$

where the length of each chip of the sequence takes 2 s, and the length of sequence is denoted by L in seconds.

We assume that the input signal is delayed by d, and hence the output signal is expressed as

$$y_1(t) = x_1(t-d) + n(t), \tag{2}$$

where $n(t)$ is a noise term that includes all the distortion effects in the wireless network, including the additive white Gaussian noise (AWGN) of the channel and domain interfaces, the multipath delay spread, the interference by all in-network and out-of-network nodes, quantization error, and sampling distortion.

The cross-correlation function is obtained by integrating the lag product of the input and output signals over the whole period of test, which is denoted by T. The cross-correlation function is denoted by $R(\tau)$ and is calculated as follows

$$R(\tau) = \frac{1}{T}\int_0^T y_1(t)x_1(t-\tau)\,dt. \tag{3}$$

The delay estimate, which is denoted by $\hat{d}$, is the value of τ that maximizes the cross-correlation function as follows

$$\hat{d} = \underset{\tau\in[0,\min\{T,L\}]}{\arg\max}\ R(\tau), \tag{4}$$

where the range $\tau \in [0, \min\{T, L\}]$ is used to account for the finite length of the binary sequence.

Moreover, we asses the time-jitter and error effects by calculating the ratio of the peak of the $R(\tau)$ to the peak of the autocorrelation function of $x_1(t)$. This ratio is denoted by β and calculated as follows

$$\beta = \frac{\max_{\tau\in[0,\min\{T,L\}]} R(\tau)}{\frac{1}{T}\int_0^T x_1^2(t)dt}. \tag{5}$$

The parameter β takes values between 0 and 1. When its value is closer to 1, it indicates that delay estimation is reliable, the variance in delay is low, and the amount of error in the received signal is small.

3.2 Error Estimation

Various types of sources can cause errors in the signals carried over industrial wireless networks. These sources include sampling, quantization, background noise, and interference. Assuming no ability to monitor packet-level measurements related to the signal, a signal-based quality estimation is used in our test method. This concept has been widely used for voice-quality measurements in order to quantify distortions in voice signals without considering the various stages of voice transmission, such as in Ref. [29] and the references therein.

To quantify the error effect on the performance of an industrial network, an arbitrary input signal $x_2(t)$ is injected at the transmitting node. The signal $x_2(t)$ is selected to be similar to practical output signals of the sensing node, for example, being a linear signal with a certain slope, or a signal with step transitions at a certain rate. The output signal $y_2(t)$ is the distorted and delayed version of $x_2(t)$. The delay is assumed to take the value of $\hat{d}$ from the first stage of the test method.

The error value is denoted by e and is evaluated using the RMS value of the difference between $y_2(t)$ and the delayed version of $x_2(t)$ as follows

$$e = \sqrt{\frac{1}{T}\int_0^T \left(y_2(t) - x_2(t-\hat{d})\right)^2 dt}. \tag{6}$$

Finally, the block diagram of the proposed test method is shown in Fig. 5.

4. Results

In this section, we illustrate the use of the proposed test method in the described testbed. We employ the system layout shown in Fig. 6, which depicts the physical locations of the nodes and not the network topology, which is not available in this work. The location of the tested wireless node has been varied in five different locations, as shown in the figure, where the distance from the gateway takes the values $\{20, 30, 40, 50, 60\}$ m. We consider two different modes of operation, which are {Single, Multiple}. In the mode with a single wireless node, the tested node operates alone in the network. In the mode with multiple wireless nodes, three other nodes operate concurrently with the tested node. These nodes transmit their own data to the gateway and are allowed to relay other data as well, based on the ISA100.11a standard. The nodes' topology is not enforced, and, hence, the nodes are allowed to self-organize using their ISA100.11a capabilities. These nodes generate traffic that is similar to the main node under study. The listed distances in the case of multiple nodes are the distances from the tested node to the gateway, while all the other nodes are fixed at the locations shown in Fig. 6. Also, due to the randomness of the channels and the ability of nodes to self-organize, the network topology and the number of hops vary over time during the testing.

The testing is done over the channels described in Sec. 2.3, which are the measured CIRs (LOS and NLOS), the IEEE802.15.4a CIRs (LOS and NLOS), the log-distance channels (LOS and NLOS), and the free space channel. Moreover, in all LOS channel models, we used a loss exponent of 1.6; for NLOS channel models, we used a loss exponent of 2.4.

In the first stage of testing, the test run time was 15 min, and we obtained two sets of results. First, in Tables 1 and 2, we show the calculated delay in single and multiple modes, respectively, where the resolution of the calculated delay is 0.5 s. Second, in Fig. 7 and Fig. 8, the value of β is shown against the distance between the tested wireless node and the gateway.

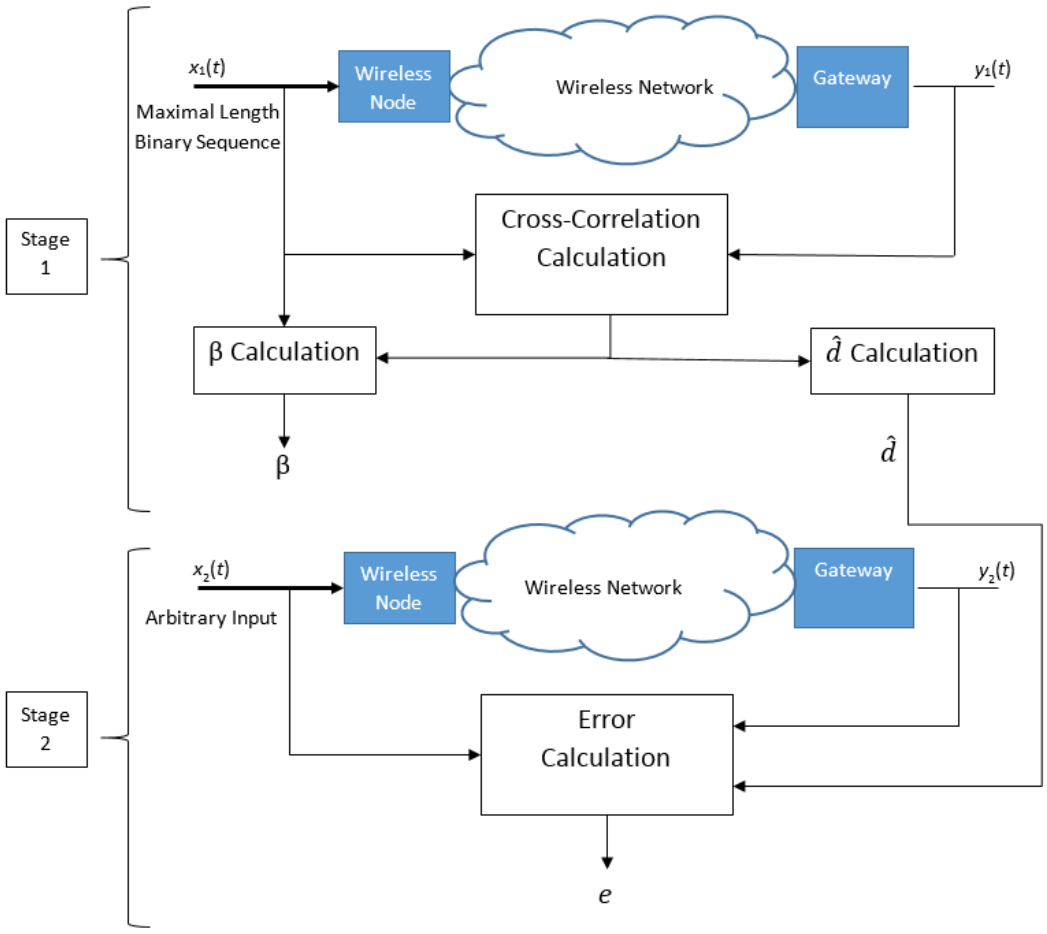

Fig. 5. The proposed test method is a two-step algorithm in which the delay estimate is fed to the error estimator.

The delay in the received signals results from various factors through the path of the transmitted signal. These factors include the transmission delay resulting from packet errors and retransmissions, processing delay at various system stages, and the buffering delay due to the Modbus protocol used in the PLC unit. From the obtained results, we note that the performance of the tested node in the single-node case is better for the first two channel models. In these two cases, the channel quality is good, and so the probability of packet loss is low. When the channel quality is worse, the delay performance of the multiple-nodes case is better than the corresponding single-node case. This happens despite having the nodes sharing the same resources because of the cooperation between the nodes and the reliable routing features of the ISA100.11a standard. We note also the increase of delays in the NLOS scenarios because of the increased channel delay spread and the increase of packet errors. In general, the observed delay of the considered testbed is limited by 4.5 s in the studied scenarios. Depending on the requirements of the applications, these delay values can be considered satisfactory. Generally, delays are almost non-distance-dependent. The only factor that may affect the delay is the processing delay for poor channels, where it takes longer for the node to recover the received signals due to poor channel quality.

The performance parameter β represents the effects of errors and delay spread in the cross-correlation function. In Fig. 7, the value of β drops for the NLOS multipath channel models in both the IEEE802.15.4a

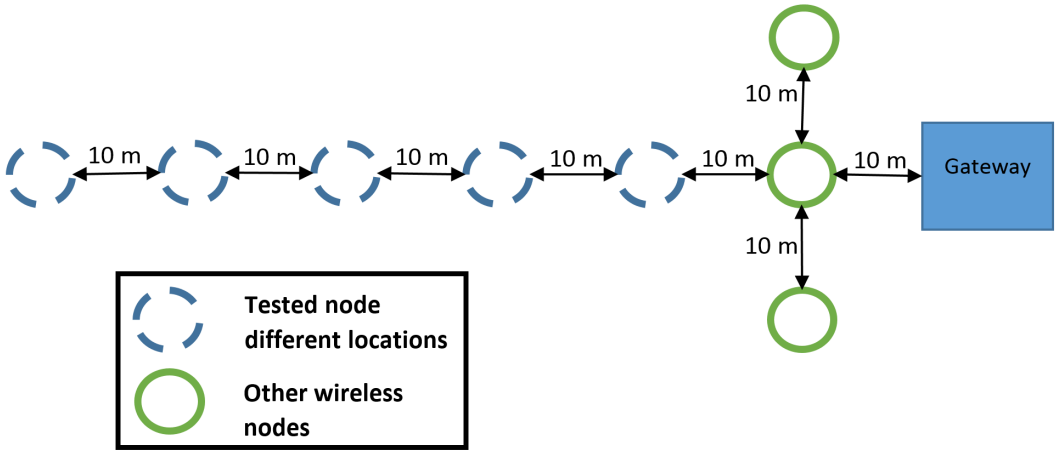

Fig. 6. The experimental procedure incrementally increases the distance between a selected node and the other nodes within the network.

Table 1. Table of the delay value in seconds against the distance for various channel models in the single-sensor case.

Channel/Distance (m)	20	30	40	50	60	Avg.
Free space	2	3.5	2.5	2	2	2.4
Log-distance LOS	3.5	3.5	2.5	2	2	2.7
Log-distance NLOS	3.5	3.5	4	4	4	3.8
IEEE802.15.4a LOS	4	4	4	4	4	4
IEEE802.15.4a NLOS	4	4	4.5	4.5	4	4.2
Measured LOS	4	4	4	4	4	4
Measured NLOS	4	4	4.5	4	4.5	4.2

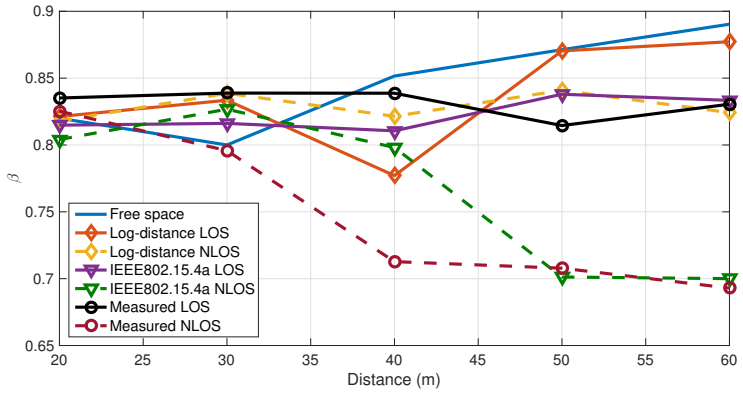

Fig. 7. The performance indicator β against the distance for various channel models in the single-sensor case.

and the measured cases. Hence, one of the major factors in degrading the performance over the tested wireless network is the severity of multipath effects, which increases for the NLOS cases. In all cases, the performances of the scenarios with multiple nodes in Fig. 8 are better than the corresponding single-node

Table 2. Table of the delay value in seconds against the distance for various channel models in the multiple-sensors case.

Channel/Distance (m)	20	30	40	50	60	Avg.
Free space	3.5	3.5	3.5	3.5	3.5	3.5
Log-distance LOS	3.5	3.5	3.5	3	3.5	3.4
Log-distance NLOS	3.5	3.5	3.5	3.5	3.5	3.5
IEEE802.15.4a LOS	3.5	3.5	3.5	3	3.5	3.4
IEEE802.15.4a NLOS	3.5	3.5	3.5	3	3	3.3
Measured LOS	4	4	4	4	4	4
Measured NLOS	3	3	3.5	4	4	3.5

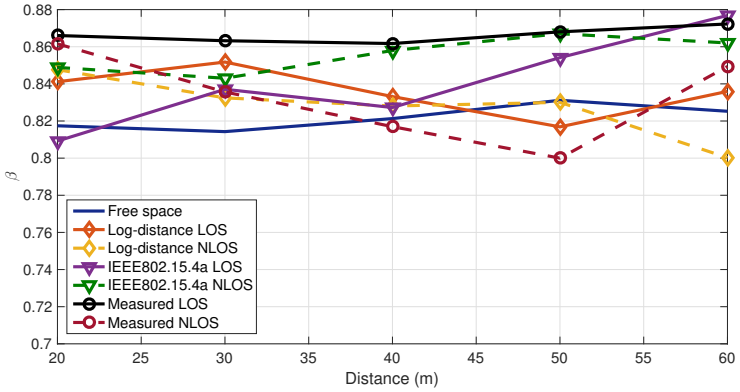

Fig. 8. The performance indicator β against the distance for various channel models in the multiple-sensors case.

cases. This shows that the impairments in the studied network resulting from the delay, the error, and the delay spread are all minimized by having the multiple cooperating wireless nodes. In Fig. 7 and Fig. 8, we found three types of curves: (1) the NLOS curves with multipath effects where β decreases when the distance increases because of the increased distortion in the received signal, (2) the free space and the log-distance LOS channel models where β increases against distance, which happen mainly due to saturation effects of the channel emulator, and (3) the rest of the channel models, where β is fixed against distance.

In the second stage of the test method, we considered two types of arbitrary input signals. First, we considered a pulse train signal with a period of 20 s and a duty cycle of 20%. The test run time was 10 min. The peak amplitude was 10 V. The error value of this type of signal can be representative of the reliability of the network in the case of transmitting step-varying signals. Second, we considered a periodic sawtooth signal with a period of 20 s and a slope of 0.5 V/s. The test run time was 50 min with random resets to average over the initial Modbus polling time. The error value of this type of signal can be representative of the reliability of the network in the case of transmitting gradually varying signals.

In Tables 3 and 4, the RMS error values of the pulse train signal are shown. As mentioned earlier, the error in the signals may result from various noise sources, such as thermal noise, channel interference, quantization error, and systemic sample phase mismatch. In the pulse train signal case, quantization effects are minimal, and so low error values occur. The main source of errors is the sampling, because the received signal duty cycle is changed significantly depending on sampling instants, where the sampling time is 1 s and the Modbus polling rate is around 2 s. More specifically, the node periodically transmits a sample of

Table 3. Table of the error values of a pulse train signal against the distance for various channel models in the single-sensor case.

Channel	20 m	30 m	40 m	50 m	60 m	Avg.
Free space	0.4578	0.3131	0.4425	0.4462	0.8169	0.4953
Log-distance LOS	0.0197	0.0735	0.3185	0.5420	0.4482	0.2804
Log-distance NLOS	0.3154	0.3185	0.2939	0.1096	0.4948	0.3065
IEEE802.15.4a LOS	0.3181	0.3291	0.4427	0.0608	0.3134	0.2928
IEEE802.15.4a NLOS	0.3046	0.1939	0.2398	0.4730	0.5834	0.3590
Measured LOS	0.7178	0.3289	0.3387	0.4484	0.5552	0.4778
Measured NLOS	0.4214	0.4629	0.5440	0.4648	0.4382	0.4663

Table 4. Table of the error values of a pulse train signal against the distance for various channel models in the multiple-sensors case.

Channel	20 m	30 m	40 m	50 m	60 m	Avg.
Free space	0.4429	0.0608	0.3208	0.3537	0.2386	0.2833
Log-distance LOS	0.0937	0.3189	0.3187	0.3822	0.0845	0.2396
Log-distance NLOS	0.3134	0.1893	0.3133	0.3135	0.1102	0.2480
IEEE802.15.4a LOS	0.3916	0.0733	0.3132	0.4464	0.4656	0.3380
IEEE802.15.4a NLOS	0.5268	0.1311	0.3811	0.2309	0.3292	0.3198
Measured LOS	0.0608	0.3233	0.5055	0.4282	0.6659	0.3967
Measured NLOS	0.4454	0.5952	0.3308	0.3204	0.1647	0.3713

measurement every 1 s. Then, the data at the gateway are buffered and polled to the PLC approximately every 2 s. The periods of these two event sequences are not synchronous. Hence, the latest received value can be delayed between 0 to 2 s for every sample. This effect adds to the randomness in delay, in addition to the transmission delay by the wireless channel. The obtained error in these measurements is slightly dependent on the wireless channels, and so there is not much difference between various error values.

Finally, we considered the RMS error values of the sawtooth signal in Fig. 9 and Fig. 10 for the single-node and the multiple-nodes cases, respectively. First, the error values are significantly larger than the corresponding values in the pulse train case. The main error contribution comes from the zero-order hold, which does not follow the signal during missed transmissions. Second, in the single-node case, the errors increase with distance as the packet error rate increases with path loss. Third, the error values in the single-node case are slightly larger than the corresponding values in the multiple-nodes case, where cooperation between nodes improves transmission reliability.

5. Conclusions

In this paper, we present a method for characterizing the performance of industrial wireless networks without the need for internal link-layer metrics. We abstracted the network and domain conversion functions of the network as a single system. We then injected a maximal length pseudorandom binary signal at one input and measured the response of the system by cross-correlating the output of the system with the pseudorandom input. The output of the cross-correlation provides an estimate of the statistical distribution of network latency for a particular node placement and network configuration. Next, we replaced the

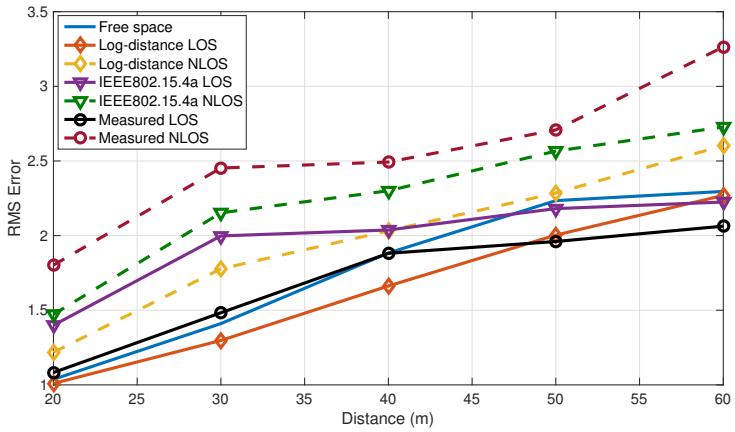

Fig. 9. The error e for a periodic sawtooth signal against the distance for various channel models in the single-sensor case.

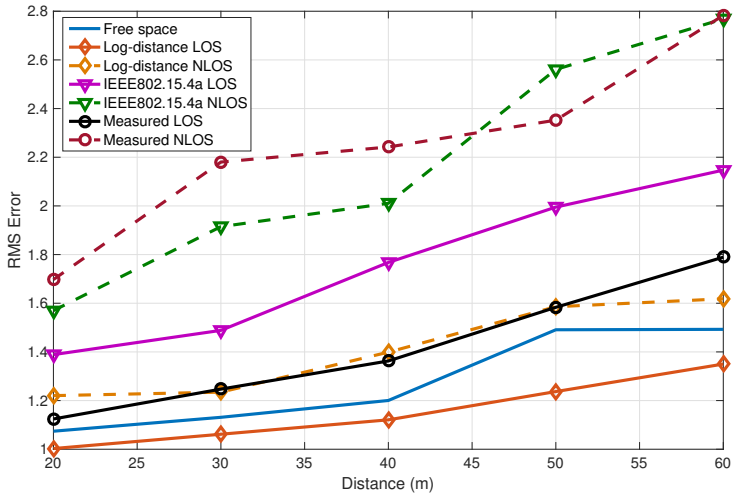

Fig. 10. The error e for a periodic sawtooth signal against the distance for various channel models in the multiple-sensors case.

pseudorandom sequence with pulse train and sawtooth functions, which are typical test signals for control systems. Using the average latency taken from the binary sequence signal correlation, we can adjust for delay and estimate the error of these signals through the network. Building an industrial testbed using ISA100.11a components and a channel emulator to consider industrial environment effects, we were able to study the proposed test method capability of assessing delay and signal-quality characteristics of a sensor or actuator input from the perspective of the controller or plant. Industrial system designers may use this method to assess network performance and to improve control system performance. This method can be applied to new installations, and, since the physical environment may change over time, it may also be used as part of a periodic maintenance plan to assess the performance of deployed wireless systems.

6. Future Work

First, the test method has to be further assessed by examination over various industrial wireless networks. This should include different hardware components, network structures, and industrial wireless technologies. Second, other performance measurements can be added to this black-box testing strategy, including jitter and error variance. In order to study new performance measures, we have to study the corresponding input test signals and the corresponding analysis tools. Finally, this method in its current form is most applicable to fixed-node systems found in continuous process factories. Our work may be extended to characterize discrete factory systems where the state of the physical process changes more rapidly. Time synchronization is an important factor in assessing network performance [30], and more work is necessary to integrate new test strategies that incorporate time synchronization into products and protocols. Moreover, in dynamic environments with changing network states, continuous monitoring approaches can be explored where the system state is captured through passive measurements of operational-level and network-level system parameters.

Disclaimer

Certain commercial equipment, instruments, or materials are identified in this paper in order to specify the experimental procedure adequately. Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that the materials or equipment identified are necessarily the best available for the purpose.

7. References

[1] Hatler M, Gurganious D, Kreegar J (2018) Wireless sensor network markets (ON World, San Diego, CA), Available at https://onworld.com/wsn/index.html.

[2] Liu Y, Candell R, Lee K, Moayeri N (2016) A simulation framework for industrial wireless networks and process control systems. *2016 IEEE World Conference on Factory Communication Systems (WFCS)*, pp 1–11. https://doi.org/10.1109/WFCS.2016.7496495

[3] Zhang L, Gao H, Kaynak O (2013) Network-induced constraints in networked control systems: A survey. *IEEE Transactions on Industrial Informatics* 9(1):403–416. https://doi.org/10.1109/TII.2012.2219540

[4] Neema H, Gohl J, Lattmann Z, Sztipanovits J, Karsai G, Neema S, Bapty T, Batteh J, Tummescheit H, Sureshkumar C (2014) Model-based integration platform for FMI co-simulation and heterogeneous simulations of cyber-physical systems. *10th International Modelica Conference*, pp 235–245.

[5] Bause F, Buchholz P, Kriege J, Vastag S (2010) A simulation environment for hierarchical process chains based on omnet++. *Simulation* 86(5-6):291–309. https://doi.org/10.1177/0037549709104236

[6] Rezha FP, Shin SY (2013) Performance evaluation of ISA100.11A industrial wireless network. *IET International Conference on Information and Communications Technologies (IETICT 2013)*, pp 587–592. https://doi.org/10.1049/cp.2013.0105

[7] Han S, Zhu X, Mok AK, Chen D, Nixon M (2011) Reliable and real-time communication in industrial wireless mesh networks. *2011 17th IEEE Real-Time and Embedded Technology and Applications Symposium*, pp 3–12. https://doi.org/10.1109/RTAS.2011.9

[8] Han S, Song J, Zhu X, Mok AK, Chen D, Nixon M, Pratt W, Gondhalekar V (2009) Wi-HTest: Compliance test suite for diagnosing devices in real-time WirelessHART network. *2009 15th IEEE Real-Time and Embedded Technology and Applications Symposium*, pp 327–336. https://doi.org/10.1109/RTAS.2009.18

[9] Wu L, Xu S, Jiang D (2015) MFAHP: A novel method on the performance evaluation of the industrial wireless networked control system. *Proceedings of the SPIE* 9794:97940E–97940E–7. https://doi.org/10.1117/12.2203479

[10] Wu LQ, Xu S (2014) Research on the performance test of wired/wireless heterogeneous industrial control network. *Frontiers of Manufacturing Science and Measuring Technology IV, Applied Mechanics and Materials* (Trans Tech Publications, Zürich, Switzerland), pp 1665–1670. https://doi.org/10.4028/www.scientific.net/AMM.599-601.1665

[11] Li T, Fei M, Hu H (2010) Performance analysis of industrial wireless network based on IEEE 802.15.4a. *Life System Modeling and Intelligent Computing*, eds Li K, Li X, Ma S, Irwin GW (Springer Berlin Heidelberg, Berlin, Heidelberg), pp 64–69. https://doi.org/10.1007/978-3-642-15853-79

[12] Li TT, Jia TG, Fei MR, Hu HS (2011) Time delay characteristic of industrial wireless networks based on IEEE 802.15.4a. *International Journal of Automation and Computing* 8(2):170. https://doi.org/10.1007/s11633-011-0570-8
[13] Zheng M, Liang W, Yu H, Xiao Y (2015) Performance analysis of the industrial wireless networks standard: WIA-PA. *Mobile Networks and Applications* 22(1):139–150. https://doi.org/10.1007/s11036-015-0647-7
[14] Cena G, Bertolotti IC, Valenzano A, Zunino C (2007) Evaluation of response times in industrial WLANs. *IEEE Transactions on Industrial Informatics* 3(3):191–201. https://doi.org/10.1109/TII.2007.903219
[15] Ferrari G, Medagliani P, Di Piazza S, Martalò M (2007) Wireless sensor networks: Performance analysis in indoor scenarios. *EURASIP Journal on Wireless Communications and Networking* 2007(1):081864. https://doi.org/10.1155/2007/81864
[16] Gong X, Trogh J, Braet Q, Tanghe E, Singh P, Plets D, Hoebeke J, Deschrijver D, Dhaene T, Martens L, Joseph W (2016) Measurement-based wireless network planning, monitoring, and reconfiguration solution for robust radio communications in indoor factories. *IET Science, Measurement Technology* 10(4):375–382. https://doi.org/10.1049/iet-smt.2015.0213
[17] Christmann D, Martinovic I, Schmitt JB (2010) Analysis of transmission properties in an indoor wireless sensor network based on a full-factorial design. *Measurement Science and Technology* 21(12):124003. https://doi.org/10.1088/0957-0233/21/12/124003
[18] Barac F, Gidlund M, Zhang T (2014) Scrutinizing bit- and symbol-errors of IEEE 802.15.4 communication in industrial environments. *IEEE Transactions on Instrumentation and Measurement* 63(7):1783–1794. https://doi.org/10.1109/TIM.2013.2293235
[19] Koutsoubelias M, Grigoropoulos N, Lalis S, Lampsas P, Katsikas S, Dimas D (2016) System support for the in situ testing of wireless sensor networks via programmable virtual onboard sensors. *IEEE Transactions on Instrumentation and Measurement* 65(4):744–753. https://doi.org/10.1109/TIM.2015.2494630
[20] Bertocco M, Gamba G, Sona A, Vitturi S (2008) Experimental characterization of wireless sensor networks for industrial applications. *IEEE Transactions on Instrumentation and Measurement* 57(8):1537–1546. https://doi.org/10.1109/TIM.2008.925344
[21] Jianyong Y, Shimin Y, Haiqing W (2004) Survey on the performance analysis of networked control systems. *2004 IEEE International Conference on Systems, Man and Cybernetics*, pp 5068–5073. https://doi.org/10.1109/ICSMC.2004.1400997
[22] RFnest (2017) Product specifications. Available at http://www.i-a-i.com/wp-content/uploads/2017/07/RFnest-Specsheet-2017.pdf.
[23] Molisch AF, Balakrishnan K, Cassioli D, Chong CC, Emami S, Fort A, Karedal J, Kunisch J, Schantz H, Schuster U, Siwiak K (2004) IEEE 802.15.4a channel model - final report, document 04/662r0. Available at http://www.ieee802.org/15/pub/TG4a.html.
[24] Karedal J, Wyne S, Almers P, Tufvesson F, Molisch AF (2004) Statistical analysis of the UWB channel in an industrial environment. *IEEE 60th Vehicular Technology Conference, (VTC2004) Fall 2004*, pp 81–85. https://doi.org/10.1109/VETECF.2004.1399930
[25] Candell R, Remley C, Quimby J, Novotny D, Curtin A, Papazian P, Koepke G, Diener J, Kashef M (2017) Industrial wireless systems: Radio propagation measurements (National Institute of Standards and Technology, Gaithersburg, MD), NIST Technical Note (TN) 1951. https://doi.org/https://doi.org/10.6028/NIST.TN.1951
[26] Mehlfuhrer C, Rupp M (2008) Approximation and resampling of tapped delay line channel models with guaranteed channel properties. *2008 IEEE International Conference on Acoustics, Speech and Signal Processing*, pp 2869–2872. https://doi.org/10.1109/ICASSP.2008.4518248
[27] Caffery JJ Jr (2000) Algorithms for radiolocation. wireless location in CDMA cellular radio systems. *Kluwer International Series in Engineering and Computer Science* 535:41–66. https://doi.org/10.1007/0-306-47329-1_4
[28] Ho KC, Chan YT, Ching PC (1993) Adaptive time-delay estimation in nonstationary signal and/or noise power environments. *IEEE Transactions on Signal Processing* 41(7):2289–2299. https://doi.org/10.1109/78.224240
[29] Falk TH, Chan WY (2009) Performance study of objective speech quality measurement for modern wireless-VoIP communications. *EURASIP Journal on Audio, Speech, and Music Processing* 2009:12:1–12:11. https://doi.org/10.1155/2009/104382
[30] Chao IC, Lee KB, Candell R, Proctor F, Shen CC, Lin SY (2015) Software-defined radio based measurement platform for wireless networks. *2015 IEEE International Symposium on Precision Clock Synchronization for Measurement, Control, and Communication (ISPCS)*, pp 7–12. https://doi.org/10.1109/ISPCS.2015.7324672

About the authors: *Mohamed Kashef is a research associate in the Advanced Network Technologies Division at NIST. Richard Candell is an electronics engineer in the Intelligent Systems Division at NIST. He leads a research project in wireless networks used for industrial control applications. Kang Lee is a research associate in the Intelligent Systems Division at NIST. The National Institute of Standards and Technology is an agency of the U.S. Department of Commerce.*