A Simulation Framework for Industrial Wireless Networks and Process Control Systems

Yongkang Liu, Richard Candell, *Senior Member, IEEE,* Kang Lee, *Fellow, IEEE,* and Nader Moayeri, *Senior Member, IEEE*

***Abstract*—Factory and process automation systems are increasingly employing information and communications technologies to facilitate data sharing and analysis in integrated control operations. Wireless connections provide flexible access to a variety of field instruments and reduce network installation and maintenance costs. This serves as an incentive for the adoption of industrial wireless networks based on standards such as the WirelessHART and ISA100.11a in factory control systems. However, process control systems vary greatly and have diverse wireless networking requirements in different applications. These requirements include deterministic transmissions in the shared wireless bandwidth, low-cost operation, long-term durability, and high reliability in the harsh radio propagation environment. It is an open question whether a generic wireless technology would meet the requirements of industrial process control. In this paper, we propose a novel simulation framework for performance evaluation of wireless networks in factory and process automation systems. We select a typical process control plant model, specifically the Tennessee Eastman Challenge (TE) Model, and define the interfaces between the process simulator and the wireless network simulator. We develop a model of the protocol stack of the WirelessHART specification in the OMNET++ simulation engine as a typical industrial wireless network. We present simulation results that validate the prospect of using WirelessHART in the TE plant, and we evaluate the impact of various wireless network configurations on the plant operation. Given its modular design, the proposed simulation framework can be easily used to evaluate the performance of other industrial wireless networks in conjunction with a variety of process control systems.**

***Index Terms*—industrial wireless networks, sensor networks, factory and process automation networks, WirelessHART, network simulation.**

I. Introduction

Cyber-physical systems (CPS) represent a paradigm shift that enables co-design of physical systems and advanced information and communications technology components to improve the effectiveness of physical systems through exchange, in-depth understanding, and exploitation of the data generated in the operations [1]. The process control and automation industry is one of the prominent application domains for CPS to improve production efficiency and eliminate potential risks and safety issues in plant operations [2]. An industrial process usually requires continuous status monitoring and timely response to any deviation from setpoints and key performance metrics. Therefore, a large number of sensors and actuators are employed by the process controller for control purposes. How to network these field instruments efficiently for process measurement and manipulation in the control system is still an ongoing research topic [3].

Wired connections are effective in supporting reliable, point-to-point communications between the controller and the field instruments. Hence, they were adopted early for process control communications, as exemplified by the HART standard [4]. However, wired connections cannot accommodate the growing demands for support of adaptive network topology and fast reconfiguration encountered in many process control systems. Instead of having to lay down miles of cables to connect hundreds of field instruments, industrial wireless communication networks provide wireless connections with customized network topology, enable plug-and-play configuration, and lower installation and maintenance costs [5]. Recently, many new industrial wireless protocols and mechanisms, such as WirelessHART [6] and ISA100.11a [7], have been proposed.

The study of industrial wireless networks is still in its infancy. Compared with Internet data services, process control operations have more rigid quality of service (QoS) requirements, including tighter message latency, lower power consumption, highly reliable transmissions in usage scenarios involving mobility and centralized data analytics [8]. As process control performance and network performance are closely coupled, a common evaluation framework for joint system design is essential and still missing. Although there exists a large and rich body of literature on control theory [9] and wireless networking [10], resulting from decades of research and development, a joint performance analysis of a system comprised of both components turns out to be difficult. On the other hand, simulation has proven to be a practical and economic approach to study the behavior of complex systems and evaluate competing solutions before field deployment [11]. The simulation-based approach has been adopted in several CPS studies dealing with smart grid systems [12] and vehicular ad hoc networks [13]. However, there is still a lack of a good simulation framework for the evaluation of industrial wireless networks in process control systems that could accommodate the diverse application domains and the unique QoS requirements encountered in this field.

This paper is among the first attempts to design industrial wireless networks in a CPS setting. We propose a simulation

Y. Liu and N. Moayeri are with Advanced Network Technologies Division, Information Technology Laboratory, National Institute of Standards and Technology, Gaithersburg, MD, USA 20899 (e-mail: {yongkang.liu, nader.moayeri}@nist.gov).

R. Candell and K. Lee are with Intelligent Systems Division, Engineering Laboratory, National Institute of Standards and Technology, Gaithersburg, MD, USA 20899 (e-mail: {richard.candell, kang.lee}@nist.gov).

framework that integrates the process control system model and the wireless network model into a unified discrete-event simulator to study the interactions between the two components and evaluate the performance under joint system design. Specifically, we select a typical chemical production plant, i.e., the Tennessee Eastman Challenge (TE) Model, as the process system model. A widely used distributed controller proposed by Ricker is employed to operate the TE plant [14]. The control process requires the transmission of a variety of process variables (PVs) between the controller and the sensors/actuators on an ongoing basis. Accordingly, a protocol stack of an industrial wireless network based on the widely used WirelessHART standard is developed to model the wireless connections in the TE plant. The interactions between the process control system, i.e., the TE process and the controller, and the industrial wireless network are coordinated by the scheduling of periodic packet transmissions that carry the PV update information. Developed in the OMNET++ simulation platform [15], the simulation framework also supports extension with the external function modules developed in other OMNET++ simulation packages. We perform a case study using the TE model to evaluate the effects of imperfect wireless transmissions on the control system performance and develop link budgets and network-assisted control. The findings of this research help engineers to identify and mitigate the weaknesses of a wirelessly networked process control system.

The remainder of the paper is organized as follows. The related work is presented in Section II. The system model is introduced in Section III. A design for the simulation framework is proposed in Section IV. A performance evaluation based on the proposed framework along with issues related to wireless network design and implementation in process control systems are presented in Section V. Concluding remarks are given in Section VI.

II. Related Work

Wireless links in the harsh process control environment suffer from severe signal propagation loss and radio frequency (RF) interference. Remley et al. measured the wireless environment in a manufacturing plant and reported the significant differences compared to the indoor office environment [16]. Also based on field measurements, other research teams report vastly different radio wave propagation characteristics in different industrial applications depending on operating frequency [17] and factory topography [18]. Based on these findings, wireless solutions providing highly reliable and deterministic transmissions in wireless links for industrial control applications are proposed. To combat the uncertainty in wireless transmissions, reliable routing is proposed that introduces redundancy by using multiple paths for each traffic flow [19]. Since most industrial wireless networks coexist in the unlicensed 2.4 GHz Industrial, Scientific, and Medical (ISM) frequency band with other wireless technologies, such as Wi-Fi, co-channel interference is another major concern in network deployment [20]. Various interference mitigation techniques proposed include employing advanced scheduling schemes to reduce the intra-system interference [21] and probing multiple channels for transmission opportunities [22]. Industrial wireless network standards, such as WirelessHART [6], [23] and ISA100.11a [7], incorporate a variety of wireless technologies at different layers of their protocol stacks to guarantee deterministic control data delivery. These technologies include multi-channel hopping, blacklisting, and mesh networking with multi-path routing. It is of great interest to decide which one to select in deploying an industrial wireless network that would also take into account constraints such as transmission power, power consumption in case of battery-operated field instruments, plant layout, and other application-specific requirements. Our design of a simulation framework to analyze the behavior and performance of an industrial wireless network in conjunction with the underlying process control problem addresses many of these issues.

Computer-based simulations have been widely used in network design and analysis, which requires repeatable comparisons among various network scenarios and alternative solutions [24]. Simulations are also widely used to evaluate complex systems, such as cyber-physical systems, by co-simulating behaviors of component systems/networks in a hierarchical High-Level Architecture (HLA) [25], [26]. Event-driven simulators, such as NS2/NS3, OPNET and OMNET++, are developed for such purposes [28], [27]. As an open source software, the OMNET++ simulator provides a flexible language to depict various network behaviors and an extensible, modular, component-based framework to support different simulation projects [15]. Based on this powerful simulation engine, two frameworks named INET and MiXiM are proposed. While INET focuses on the modular simulation of the Internet protocol functions [29], MiXiM provides wireless and mobile simulation modules [30]. However, there are no existing simulation frameworks or functional modules for industrial wireless networks in OMNET++, just as there is no framework supporting simulation of process control systems and wireless networks together. In this paper, we develop an industrial network protocol stack with the OMNET++ engine and link it with the external functional modules, including the address resolution protocol (ARP) module in the INET library and the stochastic wireless channel model template in the MiXiM library, to provide comprehensive network simulations.

A well-designed process control application model can help the wireless engineer to better understand the needs of industrial wireless communications and validate the network design before deployment. Downs and Vogel developed the TE process model as a virtual chemical plant that has many attractive features in process control study, such as centralized control, networked sensors and actuators, multivariable optimization, and performance metrics (mainly from the economic perspective) for scenarios with programmable setpoints [31]. It has been widely used in the verification of various plant control mechanisms and plant security discussions [32]. Ricker proposed several controllers for the TE model with objectives such as product rate control, quality control, and safety control [14], [33]. In these controller designs, the network connecting the controller with remote field instruments was assumed to be error-free and without

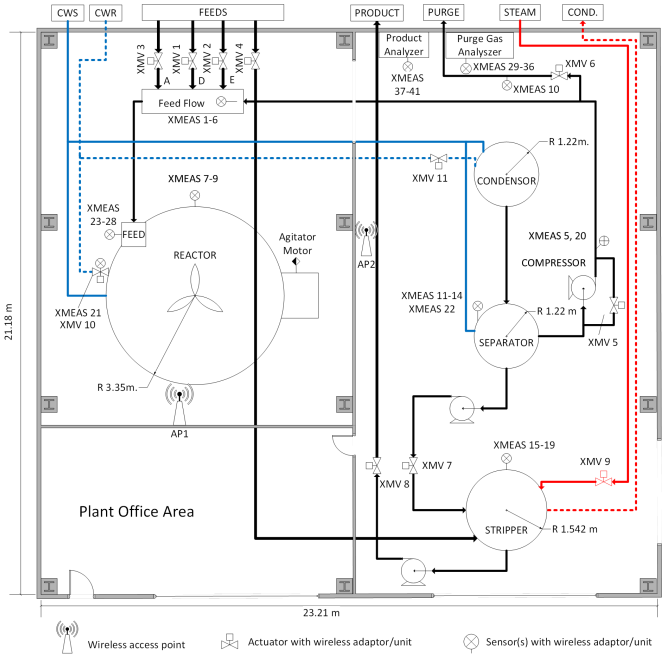


Fig. 1: A possible floor plan for the Tennessee Eastman Plant

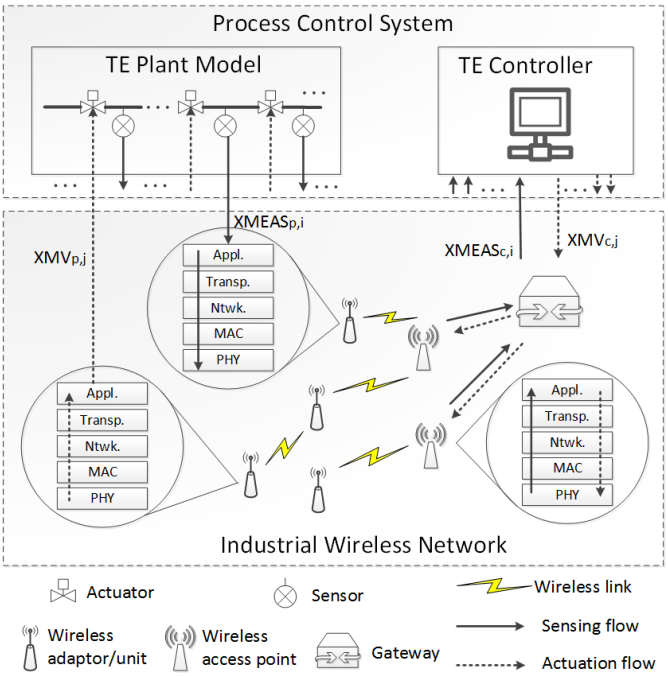


Fig. 2: Data flows in the simulation framework

any delay. When a wireless network is introduced in the plant operation, it becomes necessary to characterize the control data transmissions in the wireless links. In this paper, we adopt the TE model and Ricker's controller implemented in a wireless network setting and use the simulation approach to evaluate the effects of the wireless network on controller performance.

III. System Model

A. Factory Process Control Model

We choose the TE Model as the factory process control model in this paper [31]. Specifically, in the TE plant model, two liquid chemical products, denoted by G and H, are produced from four gaseous reactant inputs, denoted by A, C, D and E. There are one inert B and one byproduct F in the production process, both of which are also gaseous. As shown in Fig. 1, there are five operational units in the process, namely a reactor, a condenser, a vapor-liquid separator, a product stripper, and a recycle compressor. There are a total of 53 PVs available in the process, 41 of which are sensor measurements and 12 of which are manipulated variables, denoted by XMEASs and XMVs, respectively. The XMEASs indicate the instantaneous state of the process, such as temperatures, pressures, liquid levels, and chemical composition metrics. The PVs represent the control commands to various actuators, such as valve settings and coolant rates. The controller requires updates of the PV values in the plant operation on an ongoing basis to meet the production and safety requirements.

The selection of optimal controller for the TE plant is out of the scope of this paper. We choose one typical distributed controller model proposed by Ricker that uses the Euclidean solver for the TE plant control with non-linear differential equations. Interested readers are referred to [31] for the details of the reactions in this chemical process model and [14] for the controller design used in this paper.

B. Network Model in the TE Plant

As shown in Fig. 2, our industrial wireless network model consists of a gateway and several wireless access points and wireless nodes (i.e., sensors and actuators equipped with wireless adaptors). Beyond the gateway, the process control network and other network entities, e.g., security, office and asset management servers, that form the entire factory network are beyond the scope of this paper.

The gateway runs as the network manager that sets up the wireless links between the controller and the individual field instruments. The controller of the TE plant is running at the gateway and it is directly connected with all wireless access points (APs) through wired connections. The wireless nodes are distributed over the plant, either attached to the surfaces of the measured/manipulated objects or mounted on the pipes connected to them. Each wireless node is equipped with a half-duplex radio and associated with one or multiple PVs. For example, as shown in Fig. 1, the stripper-related XMEASs (XMEAS 15-19) share one wireless node at the same spot. However, each PV is allocated its own wireless bandwidth in a periodic manner to guarantee deterministic transmission within the network.

The controller requires periodic communications with the field instruments for the exchange of XMEAS and XMV PVs. To better identify different PV flows, each one carrying the XMEAS value from a sensor to the controller is denoted as a sensing flow and each one carrying the XMV value to an actuator is denoted as an actuation flow. The transmissions of PV flows in the wireless links are centrally coordinated by the gateway in such a manner that there is no interference between the wireless links in the industrial wireless network. However, alien systems may still interfere with the links of the industrial wireless network. The long-term ambient interference is incorporated in the noise level of the wireless channel model for the

industrial environment. Other intermittent interference from nearby wireless nodes can be traced and mitigated through the co-existence solutions provided for example in [21], [22]. Additional information on wireless channel characterizations in the industrial plant environments can be found in [17], [18], [34].

IV. Design of the Simulation Framework

A. Overview

We choose the OMNET++ simulation library (written in C++) to build the simulation framework as a unified discrete-event simulator. The simulation framework incorporates the process control system and the industrial wireless network in the same OMNET++ project. As shown in Fig. 2, the framework is functionally divided into a process system simulator and a network simulator. As a global function module, the process system component can be further divided into two detached modules, the TE plant and controller, respectively. The former simulates the temporal evolution of the TE process. The latter computes the control decision based on the collected XMEAS PVs. These two modules don't connect directly to exchange PV values but through their respective interfaces to the wireless network simulator. In the wireless network simulator, the wireless node (the gateway) regularly checks the memory that stores the latest XMEAS (XMV) values from the TE plant (the controller) and updates the corresponding XMEAS (XMV) values at a separate memory at the controller (the TE plant). Each time an XMEAS (XMV) is updated and its new value is transmitted via the wireless network to the controller (the TE plant), the value of the corresponding PV at the destination is updated, if the network simulator indicates that the transmission was successful. Otherwise, i.e., if the transmission does not go through due to packet loss in the wireless link, long delay caused by retransmission or rerouting along different paths, the value of the PV is not updated and remains the same at the destination. The simulation framework makes it possible to (i) evaluate the effectiveness of the controller when imperfect wireless links are used for communicating PV values, and (ii) determine which wireless technologies, if any, can support control schemes used in delay-sensitive process control applications.

There are always some challenges in integrating a continuous-time process simulation, such as TESim, with a discrete-event network simulator, particularly when the time constants for one is in the order of hours and for the other in the order of milliseconds. We integrated the two simulations at the application layer. There are three options for the integration, namely, use of socket communications, direct call of an external C++ library, and use of embedded function modules. We opted for the third option. To maximize the overall simulation efficiency and speed, given the differences in time granularity between the two component simulations, we converted the TE Model into a global C++ function module and used the application layer of each communication node (sensor, actuator, or controller) as the interface to TE Model. Another challenge was that there were no models for the time division multiple access (TDMA) medium access control (MAC) protocol used in WirelessHART or PHY layer model based on appropriate channel propagation models in the OMNET++ library. To mitigate these issues, we implemented the WirelessHART MAC protocol and we used an appropriate IEEE reference channel model in OMNET++, as described in Sections IV-D and IV-E, respectively.

We had to make some tradeoffs in developing our simulation framework. Given that our focus was on studying the effects of wireless communications on the process control system, we had to make compromises on how we modeled timing and synchronization issues. For example, any transmitted process variable is assumed to be the instantaneous value acquired from the plant. Therefore, we did not consider sampling delay or quantization error in the acquisition process. In addition, the nodes in the wireless network are assumed to be synchronized all the time, which does not model collisions or missed messages due to asynchronous wake-up of field nodes. Furthermore, one can get more realistic simulation results by using a ray tracing engine to compute the RF channel impulse response between any pair of communicating nodes at any given time. However, that would have slowed down the simulations by orders of magnitude. As a compromise, we used the IEEE channel model mentioned above, but we took into account the distance between the two nodes and whether there was a line-of-sight (LOS) or non-line-of-sight (NLOS) propagation path between them.

In the following subsections, we discuss the details of the design of the simulation framework.

B. Coordination between Process and Network Simulations

The simulation of process events, which are mainly the fixed step updates of the PV values for the plant and the controller, is independent of the network simulation. The coordination between the two components is through management of the PV memories shared between the plant (controller) and the wireless node (gateway). For example, consider $\mathrm{XMEAS}_{\mathrm{p,i}}$, the sensing flow of the i-th XMEAS in the TE plant shown in Fig. 2. At each sensing moment, the plant module updates the value of $\mathrm{XMEAS}_{\mathrm{p,i}}$ and stores it in the memory shared with the network. In the timeslot allocated for the transmission of $\mathrm{XMEAS}_{\mathrm{p,i}}$, the wireless node fetches the updated value of $\mathrm{XMEAS}_{\mathrm{p,i}}$ from the shared memory, incorporates it as the payload into an application layer message, and passes it down to the physical radio module that in turn passes it to the gateway wirelessly. Upon reception at the application layer, the gateway updates the value of $\mathrm{XMEAS}_{\mathrm{c,i}}$ in the memory shared with the controller. Similar operations take place for the actuation flow from $\mathrm{XMV}_{\mathrm{c,j}}$ at the gateway to $\mathrm{XMV}_{\mathrm{p,j}}$ at the actuator.

The simulation modules are all synchronized to the simulation clock driven by the central event queue in the simulator core. The simulator core processes one event with the current timestamp from the event queue at a time and inserts new events with present or future timestamps into the queue. The fixed step process and control updates are managed by two separate timers, each of which is reloaded to the next update moment after the latest update, as shown in Fig. 3.

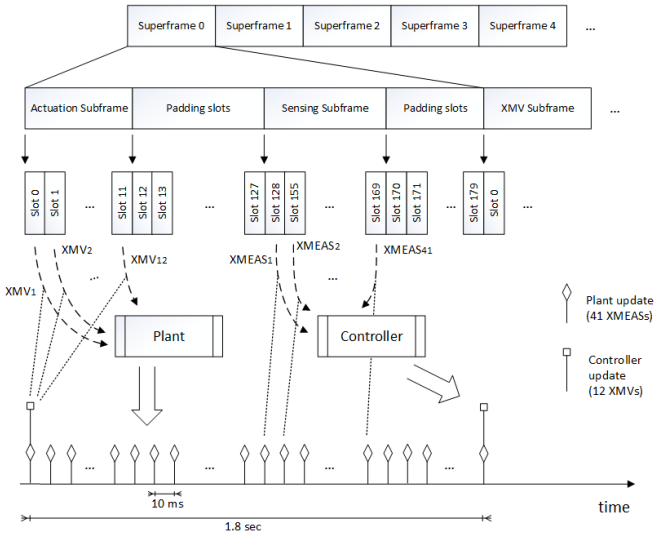


Fig. 3: Coordinations between slotted packet transmissions and PV updates

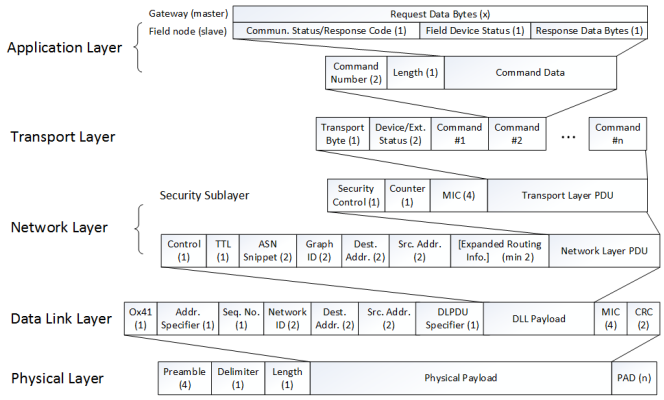


Fig. 4: WirelessHART protocol stack and inter-layer message frame structures with overhead counts

As suggested by Ricker, each PV gets one update every 1.8 second [14]. On the other hand, the network events are sorted by the timeslots and superframes along the timeline. The timeslot is the basic scheduling unit of length of 10 ms in the WirelessHART specification. One packet can be transmitted in one timeslot over a wireless link. The superframe, which is of the same length as the controller update period, i.e., 1.8 second, consists of multiple adjacent timeslots and it gets repeated periodically over time. The TDMA framing and scheduling in the WirelessHART network simulation will be discussed in more depth in Subsection IV-D.

C. WirelessHART Network Simulation

The wireless network simulator is based on the WirelessHART standard. As shown in Fig. 4, the WirelessHART protocol stack resembles the standard open systems interconnection (OSI) 7-layer protocol stack, but it consists of five layers, namely the application layer, the transport layer, the network layer, the data link layer (DLL), and the physical (PHY) layer. The detailed functional descriptions of these layers can be found in [6] and [35].

To facilitate performance evaluations, the network simulator enables key functions in individual layer modules and leaves open interfaces for future extensions. Specifically, the application layer module mainly serves as the interface with the TE process and controller modules. Command 33 (Read Variable Command) and Command 79 (Write Variable Command) of the HART communication commands are used in the simulations as the application layer messages in the update of PVs [4]. At the transport layer, multiple commands can be concatenated into one payload to reduce the control overhead and conserve bandwidth. At the network layer, the source node maintains the primary and alternative backup paths to the destination node in the routing table identified by the PV number. The mapping between the network ID and the node's MAC ID in the DLL is performed by the third party ARP module from the INET simulation package as a global function module [29]. The TDMA MAC design in the DLL module is presented in Subsection IV-D. The physical radio module is designed based on the template provided in the MiXiM wireless simulator package [30]. We have the capability to introduce new wireless channel models based on field measurement in a real plant environment. The modular design of the network simulator masks the details of the layer functions in individual protocols and encourages interchangeable reuse of the layer modules, which facilitates comparisons of various network designs using any of a number of choices at each protocol stack layer.

The information exchange between adjacent layers in the protocol stack is through messages with packet formats shown in Fig. 4. At the transmitter, e.g., the AP for the actuation flow in Fig. 2, each layer module treats the upper layer message as the payload and encapsulates it with its own control information as header to form the message packet and sends it down to the next lower layer. At the receiver, e.g., the actuator with the same flow in Fig. 2, in a bottom-up manner, each layer module acquires the information from the packet header sent by its peer layer in the AP and forwards the payload to the upper layer. Between the peer layers of two wireless nodes, the control information in the packet header, such as the routing information in the network layer and the MAC address in the DLL as shown in Fig. 4, are interpreted and used for the specific layer functions.

D. TDMA MAC Layer Design

The main function of the WirelessHART DLL is the MAC protocol which allocates the radio resources to the transmissions in wireless links. The radio resources spread over time and frequency domains.

In the time domain, WirelessHART adopts the time division multiple access (TDMA) scheme to provide timely transmissions. Other industrial wireless networks, such as ISA100.11a, use the same approach. A timeslot, of duration 10 ms, is the smallest allocation of time in the TDMA MAC that supports one handshake in a wireless link including the transmission of one MAC packet and its ACK/NACK reply. As explained in Subsection IV-B, each PV update will get its own exclusive timeslot for each of the links along the end-to-end path. Each

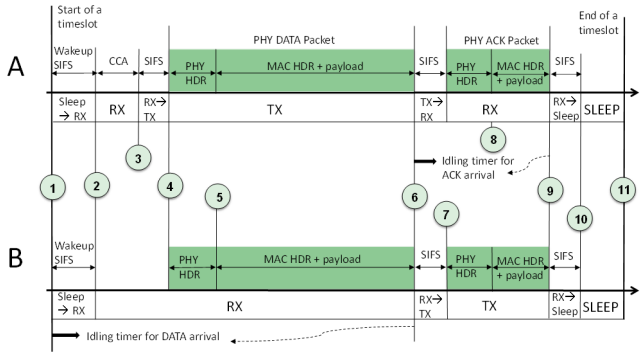


Fig. 5: Transmitter and receiver simulation events in a WirelessHART timeslot

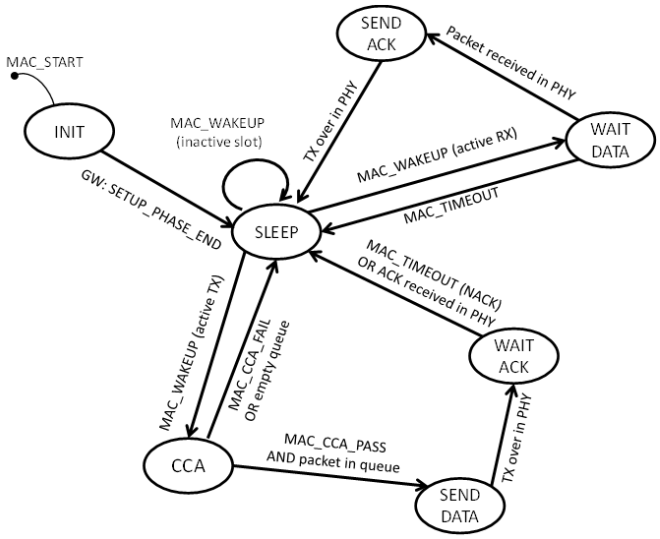


Fig. 6: Finite State Machine (FSM) representation of the WirelessHART TDMA MAC

transmission over the link is mapped to a unique timeslot with the same offset to the beginning of each superframe, which is maintained by a global schedule at the network manager. At the beginning of a timeslot, every wireless node checks the schedule. During each timeslot only the radios at the transmitting and receiving nodes are activated and they follow the procedures shown in Fig. 5. The MAC layer carries out certain tasks according to radio state and PHY layer framing and it responds to various events at different time instances. For example, consider transmission of a packet from node A to node B. At the time instance labeled 2 in Fig. 5, the transceivers at both A and B switch to the receiving state. The transceiver at A is performing carrier sensing in the clear channel assessment (CCA) state. The transceiver at B switches to the WAIT DATA state to receive the signal carrying the data packet. At the time instance labeled 6, i.e., at the completion of the data packet transmission, the transceiver at A switches to the receiving state to wait for the ACK packet and it enables the idling timer. Meanwhile, the transceiver at B stops its idling timer for the data packet and switches to transmit state to send the ACK/NACK packet. The transceiver at A will go to sleep to save energy if the idling timer expires before it is disabled by any expected packet arrival and the scheduled event of sending an ACK by B will be removed from the schedule. To depict various events and actions associated with the transceiver states and the roles various nodes play, a finite state machine for the WirelessHART MAC module is developed and shown in Fig. 6.

In the frequency domain, WirelessHART nodes work in the 2.4 GHz ISM band using the IEEE 802.15.4 radio. The WirelessHART network can employ up to 15 non-overlapping wireless channels, each with a 2 MHz bandwidth and separated from adjacent channels by a 5 MHz spacing. WirelessHART not only allocates timeslots to a given link in a periodic manner using the superframe structure, but it also uses channel hopping by assigning various channels to the same link to provide channel diversity. Specifically, the channel assigned to link l at timeslot t is given by

$$c_l(t) = T_{hop}((ASN_t + c_l) \bmod |C_a|) \tag{1}$$

where $|C_a|$ is the size of the active channel set, c_l is the original channel offset for link l, and ASN_t is the absolute slot number (ASN) of the current timeslot t since ASN 0 when the network was created. $T_{hop}(i)$ is the lookup table for channel hopping sequence with a static pseudo-random mapping between the inputs from 0 to $|C|$ [36]. Note that the set of active channels may be a proper subset of all 15 possible channels, due to the blacklisting rules that prohibit the use of some severely interfered channels.

E. Empirical Industrial Wireless Channel Model

To simulate the transmissions in the industrial environment, we employ an empirical industrial wireless channel model in the physical layer. Generally, the channel model consists of a large scale path loss model, a shadow fading component, and a small scale fading component. Specifically, as a function of the distance d between the transmitter and the receiver, the signal power P_r at the receiver can be written in the logarithmic form as

$$P_r = P_t + PL(d) \tag{2}$$

where P_t is the transmit power level, and PL is the path loss model, which can be modeled as

$$PL = PL_0 + 10n\ log_{10}(d/d_0) + X \tag{3}$$

where PL_0 is the path loss at the reference distance d_0, n is the path loss exponent, and the shadow fading component X is a Gaussian random variable in decibel, $X \sim N(0, \sigma^2)$. As noted in [34], depending on whether the link is Line-of-Sight (LOS) or Non-Line-of-Sight (NLOS), different values are used for n, σ^2 and different lookup tables are used to obtain packet error rate (PER) as a function of signal-to-noise-ratio (SNR).

We use E_b/N_0 as the link quality metric given by

$$\frac{E_b}{N_0} = \frac{C}{N} \cdot \frac{B}{R} \tag{4}$$

where C is the carrier signal power after the receiver filter but before detection including the noise figure of the receiver, N is the noise power at the receiver, B is the bandwidth and R is the channel data rate.

TABLE I: LOS/NLOS PER Table (Packet size: 64 Bytes)

E_b/N_0	$P_{e,nlos}$	$P_{e,los}$	E_b/N_0	$P_{e,nlos}$	$P_{e,los}$
0 dB	1.0000	1.0000	22 dB	0.5102	0.0606
2 dB	1.0000	1.0000	24 dB	0.4348	0.0420
4 dB	1.0000	1.0000	26 dB	0.2488	0.0308
6 dB	1.0000	1.0000	28 dB	0.1786	0.0163
8 dB	1.0000	1.0000	30 dB	0.1196	0.0106
10 dB	1.0000	0.9615	32 dB	0.0627	0.0073
12 dB	1.0000	0.7246	34 dB	0.0452	0.0041
14 dB	1.0000	0.4545	36 dB	0.0284	0.0024
16 dB	0.9804	0.3623	38 dB	0.0174	0.0016
18 dB	0.8475	0.1923	40 dB	0.0106	0.0012
20 dB	0.6667	0.1121	42 dB	0.0096	0.0000

TABLE II: Simulation Parameters

Number of XMEASs	41
Number of XMVs	12
Plant update period	1.8 s
Controller update period	1.8 s
Plant simulation time	72 hrs
Number of APs	2
timeslot	10 ms
Superframe size	180 timeslots
Number of channels	15
Per channel bandwidth	2 MHz
data rate	250 kbps
PHY Data packet size	64 Bytes
PHY ACK packet size	20 Bytes
Transmitter power	-10 dBm
Receiver noise figure	11 dB
Path loss model	IEEE industrial [34]
CCA length	192 μs
Radio wakeup time	684 μs
SIFS	192 μs

Each time a packet is transmitted, the physical layer module in the receiver calculates the value of E_b/N_0 using the link length, link type, and packet size, and then maps this value to the corresponding PER value and decides whether the packet has been received correctly or not by flipping a coin. Table I shows the PER table used in the simulator for both LOS and NLOS links.

V. Performance Evaluation

A. General Simulation Setting

We design three sets of experiments to evaluate the impact of the wireless channel on the process control system, the wireless network setup/configuration, and the coordination between wireless network and the process control system. In these experiments, the TE controller manages the plant to operate at the optimal setpoints in Mode 1, where the production rates for products G and H are the same [31]. Table II enumerates the parameters for the simulation and the typical values used in these experiments. The TE plant library and the simulation framework are maintained in the GitHub repositories [37] and [38].

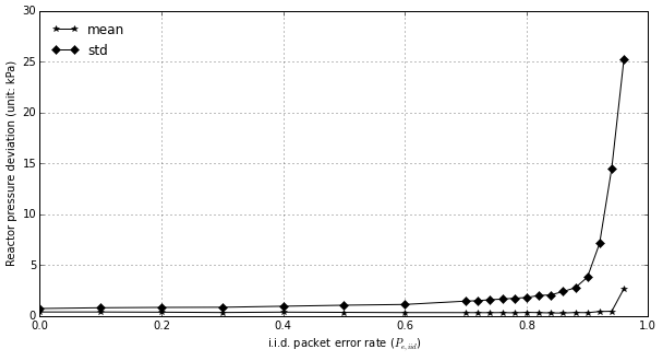


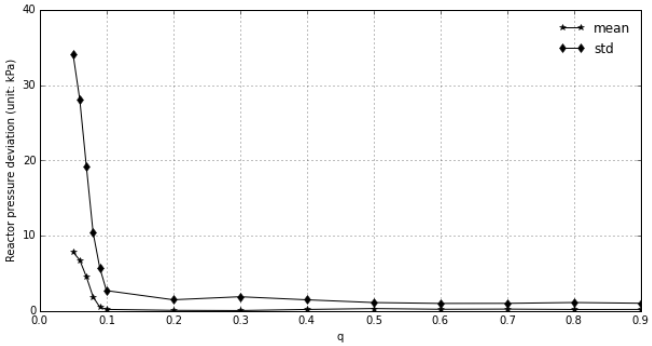
Fig. 7: Performance deviation under different packet error rates in IID channel model

B. Effects of Packet Errors on the TE Plant

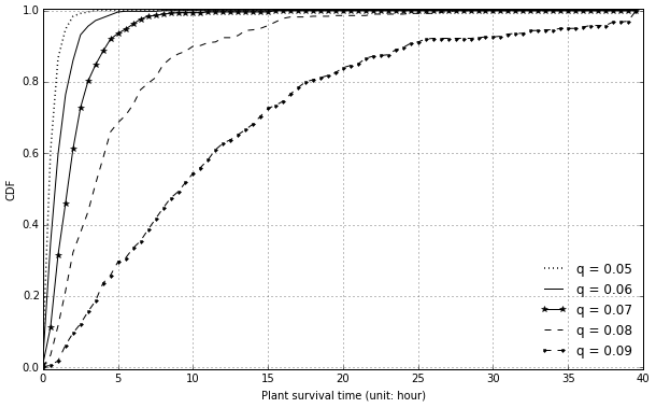
We start by studying the impact of wireless packet transmission errors on the process control performance before considering the networking issues. We assume that each field instrument is connected to the controller through a direct wireless link. Two stochastic channel models are used to model random link failures, i.e., the independent and identically distributed (IID) packet loss model and the two-state Gilbert-Elliot (GE) channel model [39], [40]. Among the many operational objectives for the TE plant, we select the reactor pressure as the performance metric because it is particularly vulnerable to imperfect control command communications. Although a higher reactor pressure is preferred because it accelerates the reactions for the products, the TE process will shut down the plant for safety reasons if the reactor pressure exceeds 3000 kPa. The setpoint for the reactor pressure is set at 2800 kPa as suggested by [14].

With the IID channel model, the wireless PV updates are statistically independent of each other and the packet error rate is the same at all times. As each PV gets updated in a superframe, a larger PER $P_{e,iid}$ makes it more likely for the packets to get impaired and dropped, which causes the controller to take more time to acquire the process status and respond to any disturbances. Fig. 7 shows the mean and standard deviation of reactor pressure from its setpoint as a function of $P_{e,iid}$. Each point in Fig. 7 represents 100 repeated experiments with random seeds. The results indicate that the reactor pressure control deviates more from the setpoint as the communication channel gets less reliable, which may result in a plant shutdown.

Next we look at the GE channel model, which is designed to model bursty losses in wireless links with two recurring states [39], [40]. In this paper, we assume that each wireless link in the experiment follows the GE model and jumps between the good state and the bad state with the transition probabilities p and q, respectively. We assume that in the good state a packet gets transmitted over the channel without any errors with 100% probability and in the bad state it gets blocked with 100% probability. Therefore, the average PER in



(a) Performance deviation



(b) CDF of plant survival time

Fig. 8: Performance of TE plant under different bursty packet losses in GE channel model ($P_{e,GE} = 0.6$)

the GE model is $P_{e,GE} = p/(p+q)$ and the average sojourn time in the good (bad) state is T/p (T/q), where T is the PV update period, i.e., 1.8 second in the Ricker's controller. A smaller q means a longer interval between successive updates over a wireless link, which reduces the agility of the controller and postpones the manipulation effort. Fig. 8a illustrates the mean and standard deviation of pressure deviation as a function of q while the average PER is kept at 0.6. Meanwhile, as there is a significant deviation of the reactor pressure when $q < 0.1$, the plant shuts down rapidly within a few hours. The smaller q is, the faster the shutdown happens. Fig. 8b verifies this with the cumulative distribution function (CDF) of the plant survival time, i.e., the time until shutdown, for different q at the same average PER of 0.6.

C. Industrial Wireless Network Setup and Configuration

In the second experiment, we evaluate the simulation framework as a supporting tool for network setup and configuration. The installation and maintenance of the wireless network in an industrial plant is usually managed by the plant information technology (IT) engineers. In case of a WirelessHART network, each wireless node is manually configured through the WirelessHART handheld field communicator [6]. Therefore, a study of the procedures in the installation and maintenance of industrial wireless networks is of special interest.

AP Site Selection

The radios of field instruments are normally installed next to the sensing/actuation parts that are typically placed at fixed locations. As the wireless links are established between the field nodes and the APs, the APs can better serve the areas they cover if their sites are carefully selected during network deployment. In this experiment, we probe for the possibility of link improvement in the simulation platform. As shown in Fig. 1, the total TE plant area can be divided into three major sectors, namely, the reaction sector (the upper left half), the product separation sector (the right half), and the office area (the lower left half). Two APs, AP1 and AP2, are deployed to serve the reaction sector and the separation sector, respectively. Each AP is associated with the wireless field instruments placed in its serving sector. Considering the availability of wired network docks and power grid supply, AP1 is mounted on the wall between the reaction sector and the office area with coordinate range ([2.5 m:11.60 m], 7 m, [1.6 m:6.5 m]) in Fig. 1, and AP2 is mounted on the wall between the reaction sector and the separation sector with coordinate range (11.75 m, [7 m:16.5 m], [1.6 m:6.5 m]). Therefore, the locations of the antennas on the mounting walls are programmable in the AP site selection procedure.

We measure the impact of the AP site on the wireless links it serves by finding the worst PER link in the coverage area as given by

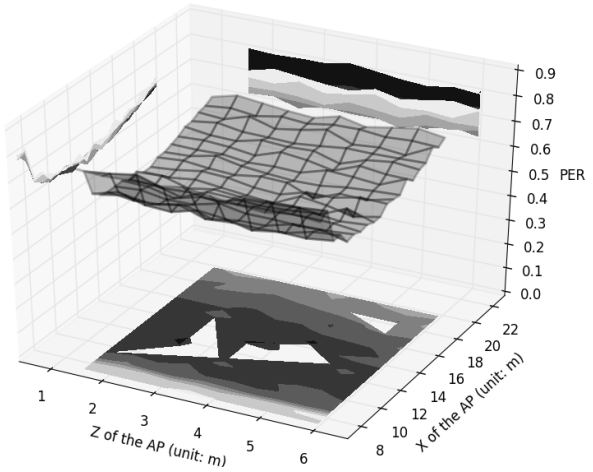
$$P_{e,j} = \max_{l \in L_j} P_{e,l} \quad for\ j \in \Theta, \tag{5}$$

where Θ is the set of all possible AP positions, L_j is the set of links between the AP at a site j and its wireless nodes, and $P_{e,l}$ is the PER for link l.

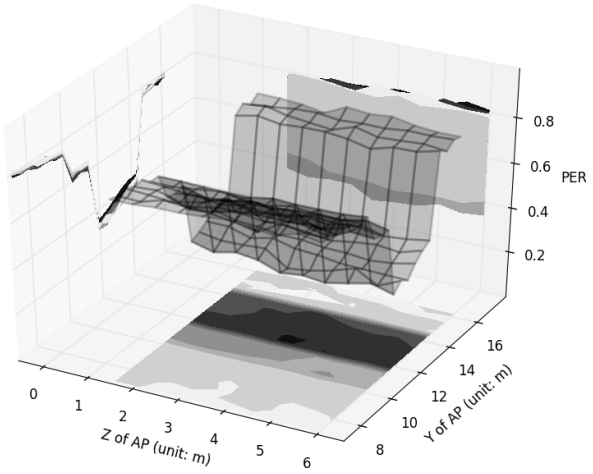
To optimize the AP placement, the objective can be written as

$$\underset{j \in \Theta}{\operatorname{argmin}}\ P_{e,j} \tag{6}$$

At each candidate position, the AP broadcasts 1000 messages at the regular transmission power and each wireless node counts the number of successful receptions, from which $P_{e,l}$ for various links are computed and reported to the network manager, which collects the $P_{e,j}$ measured at each site and decides the best AP sites in both sectors. Fig. 9 illustrates the distribution of $P_{e,j}$ for AP1and AP2 in the reaction sector and the separation sector, respectively. It is observed that the floor plan of the plant has a significant effect on the wireless links and the network performance. In the reaction sector, there is a huge reactor tank that introduces significant shadow fading in some links and causes higher PER in the links no matter where AP1 is placed on the mounting wall. The separation sector, on the other hand, houses smaller sized equipment. Hence, if AP2 is placed at certain locations, it can connect with every field instrument with a good link. As shown in Fig. 9b, when AP2 is positioned at (11.75 m, 11.5125 m, 4.54 m), it can achieve the minimum $P_{e,j}$ of 0.225. As mentioned in previous experiments, if the link PER is 0.225 or lower, the TE controller can easily manage the process and meet the objectives.



(a) Reaction sector AP1 placement



(b) Product separation sector AP2 placement

Fig. 9: Distribution of $P_{e,j}$ in the TE plant with AP placement

Link Improvements

Once the APs have been installed, "softer" mechanisms can be used in the wireless network to further enhance the links. In many cases, the link between an AP and a field instrument is NLOS, which results in higher PER and potentially requiring a number of retransmissions. Multi-hop transmissions can be enabled at the network layer by the routing function to detour the heavily faded areas. In addition, link redundancy can be introduced at the DLL by allocating retransmissions for any PV update. Specifically, a routing metric, e.g., the expected transmission count (ETX), is used to determine the best path between the wireless node and the associated AP in the sense of minimizing ETX [41]. The PV update is then transmitted to the AP along that best path. For example, in the reaction sector in Fig. 1, the feed flows, XMEAS 1-6, have poor NLOS links with AP1, and the average PER for direct connections is 0.759. Accordingly, the ETX value is $1/(1-Pe) = 4.419$, implying that on the average the direct link requires 4.419 transmissions over that many timeslots to transmit one PV update successfully. When the ETX routing is applied, the feed flows can reach AP1 via the relay at the

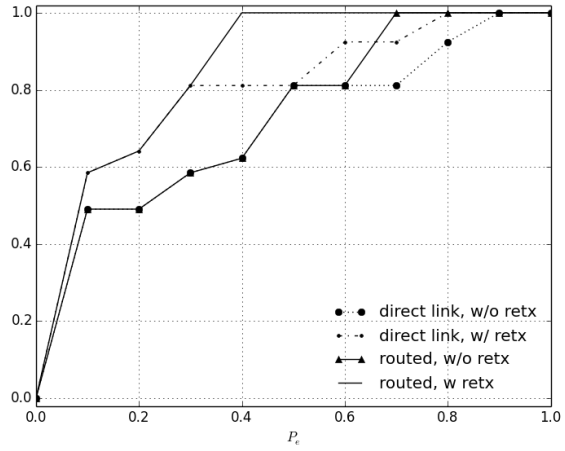
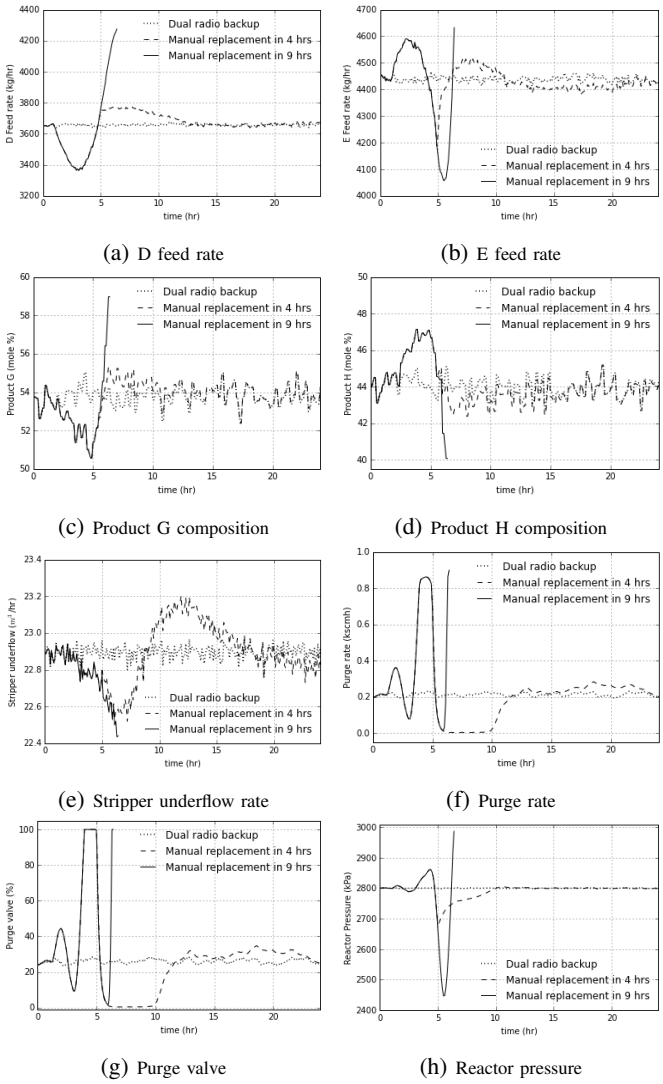


Fig. 10: Fraction PVs (out of a total of 53) for which probability of end-to-end transmission failure is smaller than or equal to P_e

wireless node that can carry the transmissions of XMEAS 23-28 and XMV 10. The ETX in the 2-hop path turns out to be 2.642. The resources allocated for each PV flow for the (re-)transmission along the path are scheduled in adjacent timeslots in each superframe using a scheduling scheme such as [42]. Fig. 10 illustrates the improvements in the PV update process by introducing retransmissions and multi-hop routing in the industrial wireless network. Therefore, full mesh-like topology in the WirelessHART network and retransmissions in the wireless links can improve the PV update performance in the TE process. When retransmissions are not used, the method of sending PV updates over direct links require 53 timeslots in each superframe and the method using multi-hop transmissions requires 63 timeslots to allow some 2-hop relay links in each transmission round. Naturally, retransmissions increase the total amount of resources required to update the PVs.

D. Effects of Network Operation on the TE Plant Performance

The developed simulation enables the interdisciplinary study of the physical process and the network. In the final experiment, we evaluate the impact of the response time to wireless network failures on the control performance. We simulate the case where a wireless link is lost due to battery problems or radio failure, which delays PV updates and in turn results in the deviation of the process from the control setpoints. Fig. 11 illustrates the simulation results in one possible case that the primary radio of the wireless node in charge of updating the feed rates, i.e., XMEAS 1-6, goes down one hour into the simulation. Several options are available to detect and fix this link problem. In the WirelessHART standard, the network manager can routinely check the field devices through Command 41 (Perform Self Test) messages. If the node does not respond to this message, the communication link may be lost. In the TE plant, such polling can be performed every minute or less frequently. The network manager can count



(a) D feed rate (b) E feed rate

(c) Product G composition (d) Product H composition

(e) Stripper underflow rate (f) Purge rate

(g) Purge valve (h) Reactor pressure

Fig. 11: PV variations in the simulations of link failure and recovery for the feed flow rate updates (XMEAS 1-6)

the non-responses over a sliding time window, e.g., 5 min, to identify the failure in the wireless link and take action to mitigate the problem by invoking the backup radio, for example.

As shown in Fig. 11, when dual radios are installed in each wireless node, the network-based link monitoring scheme can invoke the backup radio and bring the PV update back to the schedule in a few minutes. The performance degradation with respect to regular operation is minor. Compared with this embedded network solution, the alternative control-based solution needs to continuously monitor the process and send alerts upon detection of abnormal PV variations. However, as many inherent process disturbances or control system failures may also cause similar variations in the process, it usually takes longer for the plant staff to locate the problem and fix it. In the TE plant, extended absence of updated feed rates causes the TE plant to suffer from significant variation in the production, as shown in Fig. 11e, changes in product compositions, as shown in Fig. 11c and Fig. 11d, or increasing the risk that the controller shuts down the process due to high reactor pressures, as shown in Fig. 11h.

VI. Conclusions

In this paper, we have proposed a novel simulation-based evaluation framework for industrial wireless networks intended for use in process control systems. Focusing on the control-centric data flows, the framework coordinates the simulations on both sides and serves as a powerful tool in the study of the process control systems, network configuration, and the joint system design. In future work, we will study generic interface design in the framework to integrate other physical systems, such as robot control, with the wireless network for performance and safety improvements.

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.

References

[1] R. R. Rajkumar et al. "Cyber-physical systems: the next computing revolution," in *Proceedings of the ACM 47th Design Automation Conference*, 2010.

[2] J. H. Lee and J. M. Lee, "Progress and Challenges in Control of Chemical Processes," *Annu. Rev. Chem. Biomol. Eng.*, Vol. 5, No. 1, pp. 383-404, 2014.

[3] H-J K¨rber, H. Wattar and G. Scholl, "Modular wireless real-time sensor/actuator network for factory automation applications", *IEEE Transactions Industrial Informatics*, Vol. 3, No. 2, pp. 111–119, May 2007.

[4] HART Communication Foundation, "Common Practice Command Specification," HCF_SPEC-151, Rev. 8.0, Apr. 2001.

[5] J. Song et al. "WirelessHART: Applying wireless technology in real-time industrial process control", in *Proceedings of the IEEE RTAS'08*, 2008.

[6] IEC 62591 Ed. 1.0 b:2010, "Industrial Communication Networks - Wireless Communication Network and Communication Profiles - WirelessHART^{TM}," 2010.

[7] "Wireless Systems for Industrial Automation: Process Control and Related Applications", ISA-100.11a-2009 Standard, 2009.

[8] A. K. Somappa, K. Øvsthus and L. M. Kristensen, "An Industrial Perspective on Wireless Sensor Networks: A Survey of Requirements, Protocols, and Challenges," *IEEE Commun. Surv. Tutor.*, Vol. 16, No. 3, pp. 1391-1412, 2014.

[9] K. J. Åström et al. "Automatic tuning and adaptation for PID controllers-a survey," *Control Engineering Practice*, Vol. 1, No. 4, pp. 699–714, 1993.

[10] I. F. Akyildiz et al. "Wireless sensor networks: a survey," *Computer networks*, Vol. 38, No. 4, pp. 393–422, 2002.

[11] B. P. Zeigler, H. Praehofer and T. G. Kim, "Theory of modeling and simulation: integrating discrete event and continuous complex dynamic systems", Academic press, 2000.

[12] T. Godfrey et al. "Modeling smart grid applications with co-simulation," in *Proceedings of the IEEE SmartGridComm'10*, 2010.

[13] C. Sommer, R. German and F. Dressler,"Bidirectionally Coupled Network and Road Traffic Simulation for Improved IVC Analysis," *IEEE Transactions on Mobile Computing*, Vol. 10, No. 1, pp. 3–15, January 2011.

[14] N. L. Ricker, "Decentralized Control of the Tennessee Eastman Challenge Process", *J. Proc. Cont.*, Vol. 6, No. 4, pp. 205–221, 1996.

[15] "OMNET++ Discrete Event Simulator", Available at https://omnetpp.org/

[16] K. Remley et al. "NIST Tests of the Wireless Environment in Automobile Manufacturing Facilities", *NIST Technical Note 1550*, 2008.

[17] E. Tanghe et al. "The Industrial Indoor Channel: Large-Scale and Temporal Fading at 900, 2400, and 5200 MHz", *IEEE Transactions on Wireless Comm.*, Vol. 7, No. 7, pp. 2740–2751, Jul. 2008.

[18] J. Ferrer-Coll et al. "Characterisation of highly absorbent and highly reflective radio wave propagation environments in industrial applications," *IET Communications*, Vol. 6, No. 15, pp. 2404–2412, 2012.

[19] S. Han et al. "Reliable and Real-Time Communication in Industrial Wireless Mesh Networks", in *Proceedings of IEEE RTAS'11*, 2011.

[20] L. L. Bello and E. Toscano, "Coexistence issues of multiple co-located IEEE 802.15. 4/ZigBee networks running on adjacent radio channels in industrial environments", *IEEE Transactions on Industrial Informatics*, Vol. 5, No. 2, pp. 157–167, 2009.

[21] S. Lv et al. "Understanding the scheduling performance in wireless networks with successive interference cancellation," *IEEE Transactions on Mobile Computing*, Vol. 12, No. 8, pp. 1625–1639, Aug. 2013.

[22] H.T. Cheng and W. Zhuang, "Simple channel sensing order in cognitive radio networks," *IEEE Journal on Selected Areas of Communications*, Vol. 29, No. 4, April 2011.

[23] S. Petersen and S. Carlsen, "Performance evaluation of WirelessHART for Factory Automation," in *Proceerdings of IEEE ETFA'09*, pp. 1–9, 2009.

[24] B. Li, L. Nie, C. Wu, H. Gonzalez, and C. Lu, "Incorporating Emergency Alarms in Reliable Wireless Process Control," in *Proc. ICCPS'15*, 2015.

[25] H. Neema, et. al. "Model-Based Integration Platform for FMI Co-Simulation and Heterogeneous Simulations of Cyber-Physical Systems," in *Proc. 10th International Modelica Conference*, 2014.

[26] E. Galli, G. Cavarretta and S. Tucci, "HLA-OMNET++: an HLA compliant network simulation," in *Proc. DS-RT'08*, pp. 319-321, 2008.

[27] F. Bause, P. Buchholz, J. Kriege and S. Vastag, "A Simulation Environment for Hierarchical Process Chains Based on OMNeT++," *Simulation*, Vol. 86, No. 5-6, pp. 291-309, May/June 2010.

[28] P. Zand et al. "Implementation of WirelessHART in the NS-2 Simulator and Validation of Its Correctness", *Sensors*, Vol. 14, No. 5, pp. 8633–8668, May 2014.

[29] "INET Framework", Available at https://inet.omnetpp.org/

[30] A. Köpke et al. "Simulating Wireless and Mobile Networks in OMNET++ The MiXiM Vision," in *Proceedings of Simutools'08*, 2008

[31] J. J. Downs and E. F. Vogel, "A Plant-wide Industrial Process Control Problem", *Comput. Chem. Engng.*, Vol. 17, No. 3, pp. 245–255, 1993.

[32] Alvaro Cardenas et al., "Attacks Against Process Control Systems: Risk Assessment, Detection, and Response," in *Proceedings of ASIACCS'11*, Hong Kong, China, 2011.

[33] N. Lawrence Ricker. "New Simulink models of two decentralized control strategies," Available at http://depts.washington.edu/control/LARRY/TE/download.html#Multiloop

[34] A. F. Molisch et al. "IEEE 802.15.4a channel model-final report", IEEE P802 15.04, Nov. 2004.

[35] D. Chen, M. Nixon and A. Mok, "WirelessHART^{TM} Real-Time Mesh Network for Industrial Automation", Springer, 2010.

[36] K. S. J. Pister and L. Doherty, "TSMP: Time Synchronized Mesh Protocol," in *Proc. DSN'08*, Orlando, FL, USA, Nov. 2008.

[37] NIST, "Tennessee Eastman simulation," GitHub, Available at https://github.com/usnistgov/tesim, 2015.

[38] NIST, "Tennessee Simulator federated with OMNET++ networking model," GitHub, Available at https://github.com/usnistgov/tesim_omnetpp, 2015.

[39] E. N. Gilbert, "Capacity of a Burst-Noise Channel", *Bell Syst. Tech. J.*, Vol. 39, pp. 1253–1265, Sept. 1960.

[40] E. O. Elliott, "Estimates of Error Rates for Codes on Burst-Noise Channels", *Bell Syst. Tech. J.*, Vol. 42, pp. 1977–11997, Sept. 1963.

[41] S. Biswas, R. Morris, "ExOR: Opportunistic Multi-hop Routing for Wireless Networks," *ACMSIGCOMM Computer Communication Review*, Vol. 34, No. 1, pp. 133–144, 2005.

[42] A. Saifullah, Y. Xu, C. Lu and Y. Chen, "End-to-End Communication Delay Analysis in Industrial Wireless Networks", *IEEE Transactions on Computers*, Vol. 64, No. 5, pp. 1361–1374, May 2015.