Dimensioning Wireless Use Cases in Industrial Internet of Things

Yongkang Liu*, Richard Candell†, Mohamed Kashef*, Lotfi Benmohamed*

*Advanced Network Technologies Division †Intelligent Systems Division
National Institute of Standards and Technology, Gaithersburg, Maryland, USA
Email: {yongkang.liu, richard.candell, mohamed.hany, lotfi.benmohamed}@nist.gov

***Abstract*—Industrial wireless is rapidly developing to enhance data dissemination in the Industrial Internet of Things (IIoT) for leveraging the visibility, control, and safety in industrial environments. In this paper we propose a generic framework that enumerates physical and cyber factors in an IIoT use case that may impact the performance of wireless transmissions and challenge wireless system designs. These factors are discussed in a conceptually tiered structure using domain knowledge from operational technology (OT) applications, data services, and information technology (IT) infrastructures. The correlations between intra- and inter-domain factors are also discussed in search of efficient wireless design solutions. Given the diversity and variety of IIoT practices, such a framework that identifies general and specific wireless requirements in individual use cases would be of high practical value to industrial wireless design and implementation.**

***Index Terms*—Industrial Internet of Things (IIoT), industrial wireless networks.**

I. Introduction

The Industrial Internet of Things (IIoT), which makes use of generic Internet of Things (IoT) techniques [1], connects the massive number of industrial devices and enables machine-to-machine data communications in the manufacturing sector to monitor, learn, and manipulate physical processes and objects [2]. In the IIoT paradigm, communication systems play important roles that connect various industrial "things" such as sensors and actuators, and convey system status and control information within open and closed-loop processes. Compared to wired connectivity, wireless networks have advantageous features, such as connection flexibility and cost efficiency, allowing for reaching distributed nodes and serving mobile objects such as robots, raw materials, and parts moving between work cells. Wireless networks are thus becoming increasingly popular in IIoT practices.

Wireless use cases in the IIoT vary considerably in terms of traffic pattern, system operation, and deployment environment. As a result, wireless problems that are formulated in individual use cases usually differ vastly from one to another. Following the bottom-up design style that is commonly used in the literature, wireless solutions that function well under the use case conditions they were designed for may only yield limited value in different use cases. To replicate the wireless success in more plants and new applications, wireless adoption in the IIoT requires guidance from design studies to be able to identify various factors shaping wireless use cases and to weigh their impact on the wireless system design.

This paper provides a glimpse of an ongoing effort among the earliest attempts to classify wireless use cases in a named structure and identify wireless design issues that are associated with individual factors. As one of the major contributions, the proposed framework decomposes the analysis of complex IIoT use cases into separate technical domains, i.e., operational technology (OT) applications, IIoT data services, and information technology (IT) infrastructures, each of which comprises structured factors that define wireless solutions for target use cases. By adopting such a framework, OT engineers, IT administrators, and network planners are able to address the design issues in their domain expertise and collaboratively contribute to the wireless solutions.

The remainder of this paper is organized as follows. Section II reviews related work that motivates the framework design to classify various wireless use cases in industrial environments. Section III introduces the proposed framework and elaborates the relation between individual factors and their impact on wireless system design. Section IV concludes the paper and identifies further work.

II. Related Work

Research and implementation efforts have been taken in industrial wireless applications, such as collecting massive sensor data and enabling real-time control, with or without infrastructure support [3]. A number of air interfaces are introduced to build industrial wireless networks including both commercial solutions, e.g., cellular and Wi-Fi, and industrial variants, e.g., IEEE 802.15.4 time division multiple access (TDMA) radios developed for endurability and determinism [4], [5]. Radio resource management (RRM) schemes adapt network changes, such as in user traffic and radio channel characteristics, to provide reliable data services in dynamic and diverse wireless environments. Standardization efforts are also making progress in parallel to integrate wireless systems into the unified factory information architecture, such as OPC UA [6].

Diverse requirements on wireless system performance in different IIoT use cases have been observed. Such diversity mostly lies in work patterns of industrial plants, usage of the transmitted OT data, and factory IT infrastructure supports on data communication and compute resources. Some recent work

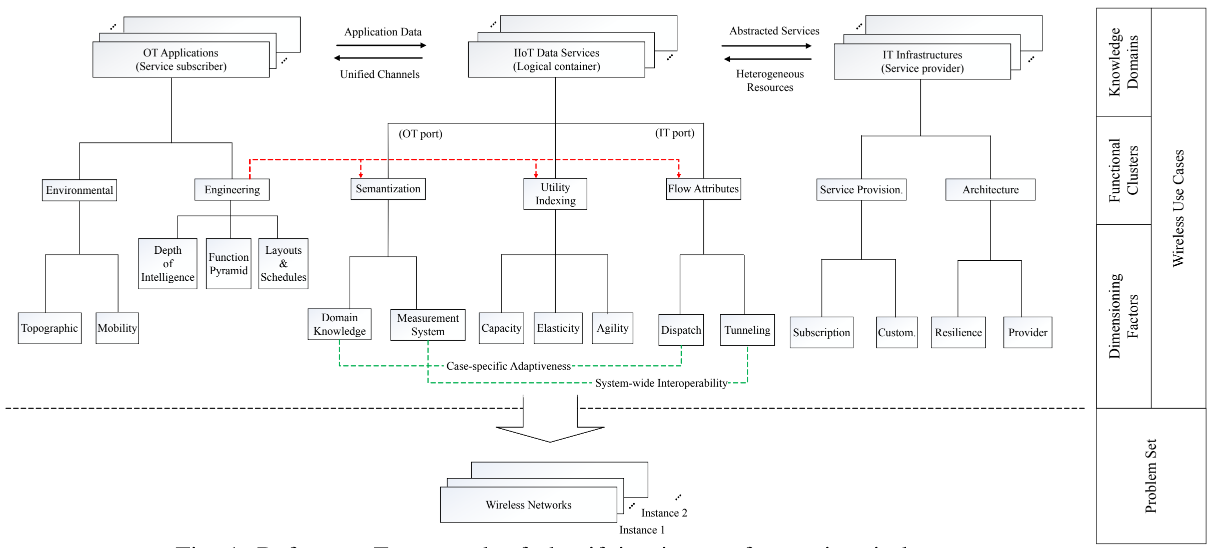

Fig. 1: Reference Framework of classifying impact factors in wireless use cases

has addressed the design of open and scalable IT platforms for generic IoT applications, such as smart grid and smart city [7]. However, IIoT deployments have unique features in terms of data structures, service requirements, and coordination between IIoT devices in factory operations, which requires tailored design principles. Moreover, as cloud computing has been in industrial control and business analytics, wireless networks are also expected to facilitate more timely and reliable communications between field devices and remote controllers [8].

Recently, some classification work has been reported in the literature that distinguishes wireless use cases by different criteria, such as the type of industrial sites, the scale of wireless connectivity, or the application of wireless data [3]. However, there is still a lack of a comprehensive review that enumerates all necessary factors in a generic use case, traces logical connections between them, and weights their values of guidance in the design of effective and efficient systems. As IIoT practices are greatly expanding the working range of wireless links and increasing the influence of wireless data services in cyber-physical systems, it is urgent to systematically revisit the classification criteria of wireless use cases. Motivated by the necessity of such a study, we propose a new dimensioning framework to classify wireless use cases and identify their particular impacts and requirements on wireless system design.

III. Factors Dimensioning Wireless Use Cases

A. *Factor Domains*

In this section, a framework is proposed that recognizes various factors in wireless use cases and elaborates their own roles in wireless system design following a layered architecture. Factors in wireless use cases, named *dimensioning factors (DF)*, are identified and organized by wireless-related functions and features in an information-centric infrastructure. The information update for OT applications is carried as various data services in the IT systems so that plant controllers and process analyzers can subscribe sensor updating services to collect data from sensors. The data can then be distributed through broadcast/multicast links along with control messages to actuators for the target applications. For each service type, the IT infrastructure will provide necessary network support on data communications, e.g., various air interfaces and communication protocols, as well as the other IT functions including data storage, computing, and IT control functions. Accordingly, factors can be represented by their roles in these services so that network planners can innovate using separate domain expertise in modularized design solutions.

Fig. 1 illustrates the proposed conceptual framework that groups DFs in three domains, i.e., *OT applications*, *IIoT data services*, and *IT infrastructures*, which form the top layer of the classification framework. Each domain further hosts the affiliated factors in functional clusters specified by domain knowledge. Before elaborating individual factors along with their respective impacts in wireless use cases, the features of the proposed framework are addressed first: (1) The domain division secures the independence and transparency of intra-domain design while offering the opportunities of inter-domain collaborations; (2) The DFs capture diverse structural features and operations of wireless use cases so that the domain expertise can be employed to address design requirements and concerns in respective dimensions; (3) A wireless use case can accommodate multiple domain instances in a complex industrial scenario, i.e., the multi-tenancy case; (4) The proposed classification framework is open and scalable, which clearly illustrates the basic rules behind wireless use cases that assist problem formulation and solution development of wireless networks in the IIoT. In the remaining part of this section, factors in each domain are enumerated with discussions to reveal their impacts on practical wireless problems.

B. *Factor Analysis in OT Domain*

Factors in the domain of OT applications address functions and activities of manufacturing systems and physical environments in a wireless use case, which vary with application tasks and plant sites. By the covered issues in the OT domain, the factors are classified into two clusters, i.e., *environmental* and *engineering* DF.

*1) **Environmental DF**:* The cluster of environmental factors depict the working environment of wireless networks and are divided into *topographic* and *mobility* factors. Topographic factors regulate the shape of the plant floor where production takes place, which covers environmental features such as (indoor/outdoor) site types, layers of floors, richness of blocks and aisles, and materials of the supporting walls and beams. The mobility factors focus on depicting the impacts of objects' movements in wireless use cases. The environmental factors are generally resource-oriented, i.e., they claim their influence on the availability and effectiveness of utilizing radio resources rather than explicitly raising requirements on data services. The topographic factors mainly function in the radio frequency (RF) environment while mobility factors shape the resource needs to support mobile nodes as discussed above.

*2) **Engineering DF**:* The other cluster of OT domain factors are engineering factors that address the OT engineering activities in the plant. Generally, these factors can be grouped into three sets which mirror the three facets in the design of industrial systems and production operations, i.e., *depth of intelligence*, *function pyramid*, and *layouts and schedules*. These three facets indicate the data-related features and operations of industrial applications in wireless use cases. Unlike environmental factors, engineering factors do not explicitly address their preference or requirements on the way of transmitting data, e.g., using wireless networks or optical communication links. Given the relative independence between OT and IT engineering efforts, the proposed framework defines a standard interface, i.e., data services, that ensures data transparency while encouraging design collaborations in cyber-physical systems. As shown in Fig. 1, engineering factors would influence wireless systems through defining and customizing various data services in wireless links, which introduces the factors in the second domain, i.e., IIoT data services.

C. Factor Analysis in Data Service Domain

Factors in the domain of data services are classified into three clusters, each of which represents one aspect of defining a data service, i.e., *data semantization*, *utility indexing*, and *flow attributes*.

*1) **Data Semantization**:* It refers to adding general markups and notifications into the formatted data so that data are annotated with domain knowledge and context information about the served applications/processes. Such add-on information, including *domain knowledge* and *measurement system*, enables different devices/systems to better interpret heterogeneous data that are shared in the IIoT. Specifically, domain knowledge is used in the semantic annotation to associate the plain data, e.g., numerical values, with their target metrics in physical processes/systems, and provides necessary system background and context information to interpret the data. Domain knowledge varies with industry and regulation. Measurement system regulates the units of measurement in target OT applications as well as identifying the representation format in the annotation.

*2) **Utility Indexing**:* Utility measures in data services share a set of perceptible performance metrics between the OT and IT systems in wireless use cases, which match various data requests of OT applications with service capabilities of IT resources at some common quality of service (QoS) level. Utility measures that depict different levels of transmission performance can be classified into three facets, i.e., *capacity*, *elasticity*, and *agility*, which regulate the performance boundaries, evaluate the change rates, and test the recognition and reaction speed to service changes, respectively. Utility measures mainly affect individual service metrics to identify the QoS in wireless transmissions. Some typical QoS metrics can be found in different service dimensions, such as the maximum flow rate (by capacity), received signal strength of edge user (by elasticity), and latency threshold (by agility).

*3) **Flow Attributes**:* Resembling the interactions between data semantization and OT applications, data services also have various flow attributes that serve as the control port to the IT infrastructure domain. As data flows may encounter conflicts between service demand and resource supply, as well as uneven distributions of IT resources, flow attributes regulate data flows in the end-to-end connections from data sources to sinks, specify the forwarding strategy at intermediate relay nodes, and check the transmission quality in each relay hop to ensure the service satisfaction over heterogeneous IT resources. There are two factors identified as flow attributes, i.e., *dispatch* and *tunneling*. Flow dispatch refers to the selection of flow paths for service data beyond a single IT system, while tunneling of data flows configures various IT resources in the end-to-end paths to provide consistent transmission performance fitting data service requirements.

Fig. 1 indicates that factors in the data service domain are indispensable in wireless use cases where they have revealed the logical connections between OT and IT systems, i.e., the OT-to-IT conversions from application data to abstract service requests and the reverse ones from heterogeneous resources to unified channels, which closes the cycle of cyber-physical system design. OT engineering factors that are identified in Section III-B influence wireless system design through data services. Meanwhile, port factors in semantization and flow attributes have addressed case-specific adaptiveness and kept system-wide interoperability in the design of IIoT data services.

D. Factor Analysis in IT Infrastructure Domain

The IT infrastructure generally comprises necessary resources, such as core network connections, compute resources, and storage resources, to support data services in collecting, distributing, and processing industrial application data. Meanwhile, it also applies various management functions and policies over these resources in a particular architecture. The impact of IT infrastructures can be identified in the operations, which are divided into two types, i.e., *service provisioning* and *architecture management*.

*1) **Service Provisioning**:* Service-oriented operations in the IT infrastructure refer to the admission, customization, and management of data services that vary diversely with their features as discussed in Section III-C. According to the processing order in a data service, these operations can be further classified into *subscription* and *customization* operations. The former one occurs before starting a new service type or adding a new service flow by user demand; and the latter one covers

TABLE I: Feature comparison between IT infrastructure options

	On-premises	Cloud (X as a Service)		
		Infrastructure (IaaS)	Platform (PaaS)	Service (SaaS)
Virtualization	Network appliances	+ Compute and storage	+ Software API	+ Software (good-to-go)
Planner	Plant IT team	Third-party cloud solution providers and network operators		
Services	End-to-end	Metal (MaaS), IaaS	PaaS	SaaS
Openness	Low	Medium	High	High
CapEx	High	Low (activation fee)	Low (activation fee)	Low/none
OpEx	Medium (utility + system updating)	Variable (subscription fee & charge per use)		
Capacity/Elasticity	Bounded	Flexible		
Scalability	Limited	Demand-specific		
Data exposure	System capacity	Site layout and shift	Traffic pattern	Information interest
Exemplary usage	Proprietary IT infrastructure	"Plug-n-play" radio access networks (RAN)	Mobile Apps	Online data subscription (e.g., air quality, utility market price)

the life cycle of active data services to allocate and adjust resources for varying service demands.

*2) **Architecture Management**:* In the IT infrastructure, architecture management operations organize IT resources and functions structurally by their physical connections (e.g., relay, bridge, and switch) and logical relations (e.g., affiliation, supplement, and competition in conceptual domains) in between. Resilience factors focus on the architectural support on IT management functions and specify the way of maintaining and orchestrating the IT system. For example, a wireless use case needs to specify its capability of using software-defined networking (SDN) and network function virtualization (NFV) technologies to tackle IT function diversity and resource heterogeneity. Provider factors address the policies that regulate the ownership and authority in the IT deployment, such as economic considerations about purchasing on-premises IT appliances and renting cloud computing and storage to build the IT architecture. As wireless networks are cooperating with factory IT architectures in IIoT practices, the wireless network design should follow the rules in the IT architecture to achieve interoperability between access and core network resources and service consistency.

E. Case Study: Process Automation

We choose a typical process automation application in a chemical production plant to demonstrate the framework usage. In the OT domain, the plant works in a typical indoor industrial RF environment with rare mobility in operations. The repeated system status measurements and actuation commands form a field control process that may work on a 24/7 schedule. As a result, such a process control application can deploy the publisher/subscriber data services to enable periodic process and control message transmissions between field nodes and the programmable logic controller (PLC). The details about the chemical process and one wireless network design based on the IEEE 802.15.4 radios can be referred to [9] and [10], respectively. When the wireless data service is integrated into the factory IT infrastructure, there would be multiple options as illustrated in Table I following the identified IT factors.

IV. Conclusions

A new comprehensive framework has been proposed in this paper which reviews the critical factors in industrial wireless use cases. Such a framework has practical value as it standardizes the design cycle of wireless systems for industrial applications and reduces the time and cost involved in customizing the design problems for different use cases. Useful directions for future work include automating the problem formulation process of industrial wireless use cases and standardizing the recommendation criteria on wireless techniques and solutions for the identified problem.

Disclaimer

References

[1] U. Sendler, *The Internet of Things: Industrie 4.0 Unleashed*, Springer Vieweg, 2017.

[2] L. Xu et al., "Internet of Things in Industries: A Survey", *IEEE Trans. Ind. Informat.*, vol. 10, no. 4, pp. 2233-2243, Nov. 2014.

[3] V. C. Gungor and G. P. Hancke, "Industrial Wireless Sensor Networks: Challenges, Design Principles, and Technical Approaches", *IEEE Trans. Ind. Electron.*, vol. 56, no. 10, pp. 4258-4265, Oct. 2009.

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

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

[6] D. Schilberg et al., "Interoperability in Smart Automation of Cyber Physical Systems", in *Industrial Internet of Things - Cybermanufacturing Systems*, S. Jeschke et al., Eds. Springer Nature, 2017, pp. 261-287.

[7] J. Gubbi et al., "Internet of Things (IoT): A vision, architectural elements, and future directions", *Future Generation Computer Syst.*, vol. 29, no. 7, pp. 1645-1660, Sept. 2013.

[8] A. Leonardo et al., "A Wireless Cloud Network Platform for Industrial Process Automation: Critical Data Publishing and Distributed Sensing", *IEEE Trans. Instru. Meas.*, vol. 66, no. 4, pp. 592–603, Apr. 2017.

[9] 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.

[10] Y. Liu, R. Candell, K. Lee, and N. Moayeri, "A simulation framework for industrial wireless networks and process control systems," in *Proc. IEEE WFCS'16*, May 2016, pp. 111.