IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received July 28, 2020, accepted August 21, 2020, date of publication August 26, 2020, date of current version September 9, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3019665

A Survey on Industrial Internet With ISA100 Wireless

THEOFANIS P. RAPTIS, ANDREA PASSARELLA, AND MARCO CONTI
Institute of Informatics and Telematics, National Research Council, 56124 Pisa, Italy

Corresponding author: Theofanis P. Raptis (theofanis.raptis@iit.cnr.it)

This work was supported in part by the European Commission through the H2020 INFRAIA-RIA Project SoBigData++: European Integrated Infrastructure for Social Mining and Big Data Analytics under Grant 871042, and in part by the H2020 INFRADEV Project SLICES-DS Scientific Large-scale Infrastructure for Computing Communication Experimental Studies—Design Study under Grant 951850.

ABSTRACT We present a detailed survey of the literature on the ISA100 Wireless industrial Internet standard (also known as ISA100.11a or IEC 62734). ISA100 Wireless is the IEEE 802.15.4-compatible wireless networking standard ''Wireless Systems for Industrial Automation: Process Control and Related Applications''. It features technologies such as 6LoWPAN, which renders it ideal for industrial Internet edge applications. The survey focuses on the state of the art research results in the frame of ISA100 Wireless from a holistic point of view, including aspects like communication optimization, routing mechanisms, real-time control, energy management and security. Additionally, we present a set of reference works on the related deployments around the globe (experimental testbeds and real-terrain installations), as well as of the comparison to and co-existence with another highly relevant industrial standard, WirelessHART. We conclude by discussing a set of open research challenges.

INDEX TERMS Industry 4.0, industrial internet, industrial control, Internet of Things, manufacturing automation, process control, wireless sensor networks.

I. INTRODUCTION

The Industry 4.0 paradigm is a many-faceted approach involving aspects as diverse as robotics, automation, wireless networking, artificial intelligence, human-in-the-loop design, data management, and digital twins. A key aspect in Industry 4.0 is the possibility to interconnect industrial systems at different scales (shopfloor, factory, enterprise) through digital technologies, enabled by the pervasiveness of Internet connectivity. In principle, any physical object can be represented by a digital twin, making the distinction between the physical and cyber worlds blurring (cyber-physical convergence), and enabling unprecedented flexibility in terms of control and optimization processes [1].

Data flows are one of the key enablers of this convergence, as they allow the linking between the physical objects and their counterparts in the cyber world. This consolidates the advanced integration of industrial machines and the new generation of data distribution over the Internet, it introduces a new interconnectivity of industrial resources, network elements and diverse data types [2]. However, technical challenges have appeared, specifically related to efficient and standardized connectivity and communication [3], routing mechanisms [4], real-time control [5], energy management [6], and security administration [7]. Intelligent industrial control systems operate over proprietary protocols and are distributed throughout the entire IPv4 and IPv6 spaces. The main Industry 4.0 requirements introduce the necessity for high reliability, fast response times, and exploitation of computational resources at the edge of the network, with efficient data management, computation and communication [8]. Moreover, as industrial stakeholders proceed to establishing data-oriented cognitive robotics and modular manufacturing systems, converting their manufacturing processes to include more competitive and adaptive features, they face the issue of seamless interconnection of the physical automation processes with their digital counter parts. This issue can increase the required costs and difficulties with respect to network planning and management [9].

Wireless technologies are now playing a key role in this cyber-physical convergence and the industrial data management [10]. Wired industrial control systems necessitate expensive communication equipment (such as cables) to be mounted and maintained. Moreover, cabling significantly

The associate editor coordinating the review of this manuscript and approving it for publication was Nitin Nitin.

limits the flexibility of use of many objects. Therefore, wired deployments are increasingly replaced by wireless technologies [9], and there is an emerging need for standardized, cost-efficient wireless industrial technologies which enable significant savings and satisfy Industry 4.0 requirements by optimizing the management of industrial spaces [11]. IEEE 802.15.4 is a suitable technology for a wide range of wireless industrial use cases, thanks to its cost-efficient energy consumption, satisfying communication range, sufficient scalability, and mesh networking reliability. Its physical layer is able to support short/medium range communications and provides industrial stakeholders with an option for low cost purchase and maintenance, low data rates and reduced energy consumption. Moreover, it is already supported by many commercial off-the-shelf integrated circuits [12].

In response to the emerging industrial requirements, there are some working groups with the purpose of defining and establishing industrial wireless-technology standards for diverse use cases. Due to the widespread acceptance of IEEE 802.15.4 amongst industrial users and vendors, the majority of those working groups have adopted the IEEE 802.15.4 physical layer. One of those working groups is the International Society of Automation (ISA), which has defined the ISA100 Wireless standard. ISA100 Wireless is one of the candidate standards which are potentially able to address the strict requirements on monitoring, control, reliability and safety imposed by Industry 4.0 [13]. ISA100 Wireless defines the protocol stack, system management and security functions for use over low-power, low-rate wireless networks. On the other hand, it does not specify a process automation protocol application layer or an interface to an existing protocol. It only specifies tools for constructing an interface [14].

A. CONTRIBUTION AND ROADMAP

This survey article reports on the research literature over the period 2009-2020 on the ISA100 Wireless standard. The article targets at filling the gap of a dedicated ISA100 Wireless survey and taxonomy of improvements and approaches (e.g., for data management) built on top of the standard, instead of extensively describing the standard and comparing it to other related solutions. The motivation behind our methodology is to provide the readers coming from both the ICT and manufacturing and control fields with an overview of the existing focus of the literature, as well as some open research challenges. The article roadmap is displayed in Fig. 1. Although there are already some surveys and review articles which partially cover some aspects of the literature, the current article is necessary due to a number of reasons, which for easiness of presentation are provided in section II, together with a comparison to other related survey/review articles. In section III, we introduce a short description of the ISA100 Wireless standard, focusing on its structural characteristics, the application on critical control use cases and the similarities and differences with other related standards, most notably WirelessHART. Section IV presents the core improvements of the ISA100 Wireless mechanisms and services on top of it

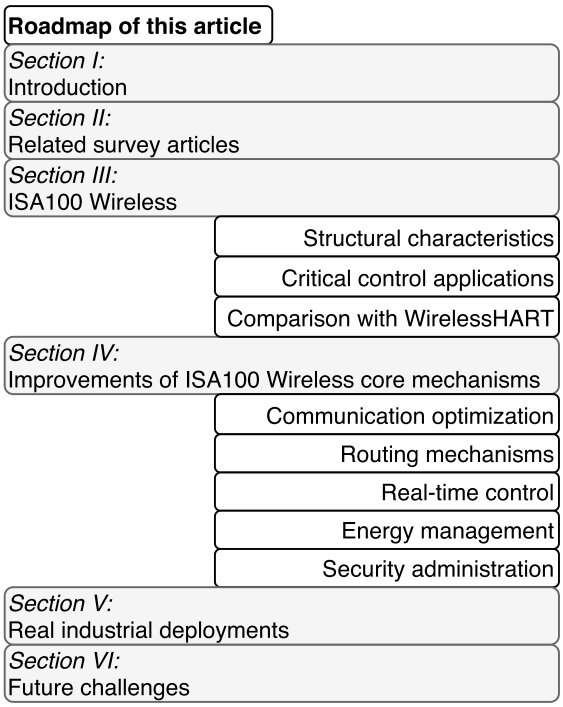

FIGURE 1. Article roadmap.

that have been presented in the literature so far. We grouped those improvements and services in five fundamental categories; communication optimization, routing mechanisms, real-time control and security administration. In section V, we present some practical considerations on ISA100 Wireless which have been addressed by a considerably large portion of the literature and we discuss a set of works which demonstrate actual industrial deployments across the globe. Finally, in section VI we outline some open research challenges that we identified after the literature review.

II. RELATED SURVEY ARTICLES

There are already some articles which partially cover some topics presented in our article. This section presents a review of the most interesting works. In the first part of the section we describe the main content of each work. Then, we highlight the difference between them and our paper, and the gaps that our paper fills in this landscape. Table 1 displays the confrontation with those works which focus on ISA100 Wireless among other technologies.

We note that a closely related research field is the 5G ultra-low latency (ULL) and ultra-reliable low-latency communication (URLLC). Although these 5G ULL and 5G URLLC techniques are not (yet) directly applicable for most industrial applications, the 5G ULL and 5G URLLC techniques are getting better and better and may soon find their way into the industrial domain. Therefore, the interested reader can get informed about this related area through a series of articles, such as [15], which presents a survey of the IEEE TSN and IETF DetNet standards, [16], which presents a survey on the emerging technologies to achieve

TABLE 1. Comparison with existing survey/review articles which include ISA100 Wireless among other standards.

	current	[19]	[12]	[20]	[21]	[22]	[23]	[24]	[11]
Communication	✓	✓			✓		✓		
Routing	✓	✓	✓		✓	✓			✓
Real-time control	✓				✓			✓	
Security	✓	✓	✓			✓		✓	✓
Energy	✓	✓			✓				✓
Comparisons	✓	✓	✓	✓	✓	✓	✓	✓	
Implementations	✓	✓		✓					
ISA100-exclusive survey	✓								
ISA100-specific research directions	✓								
Coverage up to	2020	2018	2016	2015	2012	2010			2009

ULL considering elements such as software defined networks, network function virtualization, caching, and mobile edge computing, [17], which discusses the design challenges related to URLLC use cases and on the available technology components from 3GPP Rel-15 and potential ones from Rel-16, as well as [18] which describes the functionality of both the NR and LTE radio interfaces to provide URLLC services.

A first review article is [11], the aim of which is to give a presentation of the state of the art on industrial wireless networks and lay down the research challenges of this topic. The authors first introduce general technical issues and design considerations for industrial wireless in terms of software (SW) development, hardware (HW) implementation and system architecture. In particular, they focus on radio frequency (RF) and energy harvesting technologies, as well as cross-layer designs and implementations. The relevance of this survey with our paper comes in the second part, in which wireless standards are presented (including ISA100 Wireless) for the industrial operators, who plan to use related technologies for automation use cases.

In [22], the authors review Zigbee PRO, WirelessHART, and ISA100 Wireless and present their security mechanisms. They identify a group of threats and possible attack schemes in the routing layer, and they give some recommendations as well as countermeasures to better fortify industrial deployments.

In [19], the authors discuss implementation targets, challenges, and methods for industrial wireless networks. They also present an extended outline of popular industrial protocols and standards, including ISA100 Wireless, along with a report on useful HW designs and selected energy harvesting solutions.

In [23], the authors observe that the coexistence problem between IEEE 802.15.4 based networks has been deeply explored when it comes to other non-IEEE 802.15.4 standards. Also that the problem has been further investigated in the scope of ISA100 Wireless, as well as other standards like Zigbee and WirelessHART. Therefore, the authors report on the traditional techniques in this field, and present the approaches followed by different works. Then, based on their classification, they present some open challenges of future investigation.

In [24], the authors first select different wireless industrial standards - ISA100 Wireless, WISA (Wireless Interface for Sensors and Actuators), WirelessHART, ZigBee, ZigBee PRO, IEEE 802.15.4e - and afterwards write a report on their main attributes. Afterwards, they focus on automation use cases to understand the quality of service requirements and classify the presented standards according to the requirements. Then, they carry out an investigation of possible threats targeting pertinent security requirements and they explore if and how the presented standards satisfy the security requirements.

Another paper which surveys existing popular industrial wireless standards is [21] (ISA Wireless, WISA, WirelessHART, ZigBee PRO, IEEE 802.15.4e, WIA-PA, TSMP). This paper reports on the advantages and the disadvantages of each standard and investigates the extent to which every standard can satisfy the strict requirements of Industry 4.0. Furthermore, it summarizes research approaches which target real-time critical automation use cases. The paper also presents some key open challenges existing on the physical layer of industrial wireless which have yet to be tackled in order to ensure the resilient utilization of industrial wireless standards in monitoring and control use cases.

In [12], the authors discuss and comparatively examine key and architectural aspects of ISA100 Wireless, ZigBee, WirelessHART, and WIA-PA. The peculiarities of each standard are exposed and design considerations are highlighted. The authors also present and confront the pros and cons of each standard at each ISO/OSI layer. With consideration of the functionality and operating mechanisms of the standards, the authors examine also their suitability to satisfy the related industrial requirements.

In [20], the authors try to identify standards which are able to support reliable communication in electrical substations under impulsive noise. They report on several standards - ISA100 Wireless, 6LoWPAN, ZigBee, WirelessHART, OCARI (Open Communication protocol for Ad hoc Reliable industrial Instrumentation) - and they note that the lower layer attributes are similar for all the selected standards (IEEE 802.15.4), with considerable structural diversity existing in the higher layers. Finally, the authors provide a review of characteristic properties of impulsive noise in electrical

substations (for example, amplitude, duration and rising time, impulse rate).

Although the aforementioned papers provide a detailed introduction to the current state of the art on industrial wireless networking, there are important gaps in the literature that our paper fills. Specifically:

- The vast majority of the existing surveys provide generic guidelines, applications and challenges for industrial wireless networking, highlighting them also from the point of view of ISA100 Wireless, among other standards as well. On the contrary, to the best of our knowledge, the current paper is the first dedicated survey on ISA100 Wireless.
- Most of the other existing surveys do not serve as exhaustive surveys of the work that has been done on ISA100 Wireless; they rather act as critical reviews on this and other standards, and discuss the foundations of industrial inter-networking. On the contrary, the current paper acts as an exhaustive literature survey on the technical works that have addressed, improved or compared with ISA100 Wireless.
- As shown in Table 1, the current paper covers a holistic collection of focus areas that – to the best of our knowledge – have never been addressed collaboratively in the past by a single paper. Additionally, due to the fact that the rest of the works presented in this paper have been published 2-11 years ago, the current paper provides a more up-to-date review of existing literature and the latest developments in the field.

III. ISA100 WIRELESS

ISA is developing standards for industrial automation. An ISA committee, which is called ISA100, is responsible for the development of industrial standards and recommended practices targeting technological implementations of automation and control wireless systems. The ISA100 committee has established a set of industrial wireless standards called ISA100 [25]. The ISA100 set targets at standardization compatible with networks for the industrial manufacturing environment. The ISA100 Wireless Compliance Institute (WCI), a member of the Automation Standards Compliance Institute (ASCI), consolidates wireless products and system specifications and processes used by the ISA100 wireless set. Manufacturing and automation control system stakeholders which participate in WCI, are creating and testing standardized, industrial wireless solutions. WCI owns the ''ISA100 Wireless Compliant'' certification and is testing independently wireless devices in order to verify that they conform to the ISA100 Wireless standard [26]. When adopting the ''ISA100 Wireless Compliant'' certification, different industrial stakeholders can work under the same technical specifications and increase the mutual interoperability on their wireless communication platforms.

The ISA100 Wireless standard has been developed to be a universal standardized solution for industrial wireless networks. ISA100 Wireless targets at ensuring reliable and secure services for a wide number of applications, such as supervisory control, alerting, open and closed loop control, as well as non-critical monitoring [19]. Within the frame of the ISA100 Wireless, the main specification definitions include the protocol stack, the system administration, the details regarding the network gateway implementation and the security considerations for low data rate wireless devices (both stationary and mobile) which enable low power consumption. ISA100 Wireless focuses on addressing the emerging Industry 4.0 requirements, such as monitoring and process control where end-to-end latencies at the order of 100ms can be achieved, with additional potential for even shorter latencies. In order to achieve this objective, it manages to address interference found in harsh industrial environments with robust performance, even under the presence of various other standardized wireless communication solutions. Additionally (as it will also be demonstrated by some works presented in the following sections), it can successfully coexist with diverse wireless devices in the shopfloor, like smartphones, or IEEE 802.15x, IEEE 802.11x and IEEE 802.16x, enabled devices. Finally, ISA100 Wireless enables ISA100 devices interoperability and does not explicitly specify the performance characteristics of shopfloor wireless security. Instead, the shopfloor security design is left to the end user's side of implementation [27].

ISA100 Wireless was approved as an international standard in 2011 (ISA/ANSI ISA100 Wireless-2011). Due to the fact that IEC standards hold a better visibility and adoption outside the US, ISA100 Wireless received IEC approval in 2014 as ISO/IEC 62734. In this form, the standard is able to define the specifications complying to the OSI Basic Reference Model (ISO/IEC 7498-1), and, according to [20], the manufacturers of ISA100 Wireless did not provide to the standard a built-in interoperability. However, due to the fact that the standard can employ 6LoWPAN in order to handle IPv6 (Internet) traffic, it is also able to achieve compatibility with the industrial Internet.

A. STRUCTURAL CHARACTERISTICS

A very nice introduction to the structural characteristics of ISA100 Wireless is provided in [12] and [28]. Security aspects are extensively covered in [22]. We outline here some basic features, for the reader's convenience. The ISA100 Wireless network architecture is depicted in Fig. 2. For a deeper discussion, the reader can refer to [12]. In Table 2, we juxtapose the ISA100 Wireless stack with the ISO/OSI stack and we note that the OSI presentation and session layers are absent in the ISA100 Wireless stack.

- ISA100 Wireless uses in the physical layer the IEEE 802.15.4 standard [29], which uses 27 channels, numbered 0-26, at three different frequency bands. The 2.4 GHz band (which is globally unlicensed for almost all channels) is assigned to channels 11-26, with 5 MHz channel spacing. Consequently, ISA100 Wireless is using the 2.4 GHz frequency band.

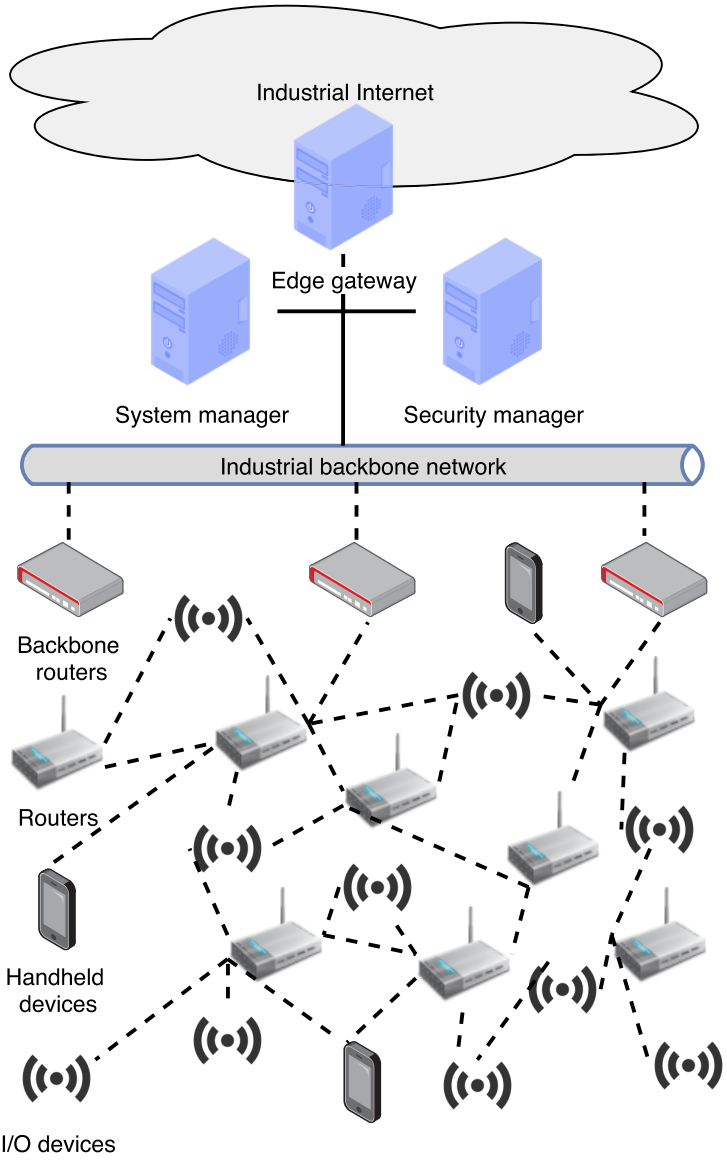

FIGURE 2. ISA100 Wireless network architecture.

TABLE 2. ISA100 Wireless functionalities (based on info extracted from [12], [19]).

ISO/OSI Layer	ISA100 Wireless Functionality
Application	Object-oriented, pub/sub, client/server, native/non-native, tunelling
Presentation	-
Session	-
Transport	connectionless, optional security (symmetric/assymetric)
Network	6LoWPAN, graph/source/superframe routing, fragmentation
Data link	CSMA/CA, TSMP, channel hopping (slotted, frequency), blacklisting
Physical	IEEE 802.15.4 (2.4 GHz)

- ISA100 Wireless uses, on top of the IEEE 802.15.4 physical layer, a modified version of the IEEE 802.15.4 MAC layer, by enhancing the MAC with added functions like channel hopping, communication with time slots and synchronized TDMA/CSMA in the domain of time.
- In fact, logically, the aforementioned functions are usually part of the MAC layer, but are implemented in the data link layer. Source, graph and superframe routing mechanisms are also implemented in the data link layer. This is due to the fact that network layer routing is reserved for the backbone router.
- The ISA100 Wireless network and transport layers are compatible with 6LoWPAN [30], which introduces IPv6 (Internet) packets in IEEE 802.15.4 networks and deals with requirements of the industrial Internet. This feature

is particularly important, as an emerging trend of Industry 4.0 is the gradual replacement of existing wired networks; therefore industrial wireless installments with Internet compatibility are beneficial, especially when they are able to provide interplay with wired solutions, such as industrial Ethernet. Additionally, the network layer supports fragmentation for transmitting large amounts of data.
- The application layer of ISA100 Wireless introduces a reference tunneling mechanism which enables the wireless devices to encapsulate legacy protocols. Object-orientation also further promotes the interoperability between diverse commercial devices.

ISA100 Wireless defines two main classes of devices, Field Devices and Backbone Devices, and two dedicated manager devices: the system manager and the security manager [31]. The system manager is in charge of the network resource management and communication provisioning, while the security manager implements the security design which depends on the security policy adopted. The class of Field Devices can support wireless devices with or without routing capability. For example, a mobile, handheld device such as a smartphone can be classified as a field device without routing capability. The indicative objective of such a device in the network is to associate with a routing device and to pass important data or monitor and analyze the network traffic. Roaming of mobile devices is out of the scope of ISA100 Wireless. Backbone devices in the network are provided with high energy supplies and are thus constantly powered, while field devices typically have limited battery capacity. The system manager acts as the global network clock and manages the time and time-synchronization information. ISA100 Wireless is assumed to implement a TDMA mesh topology resulting in a robustly centralized and relatively stationary deployment, targeting related Industry 4.0 applications. Although the star topology can be supported by the standard, the mesh topology is preferable since it offers greater reliability, as well as a greater capacity for external interference management. ISA100 Wireless central data management (through the system manager), achieves dynamic topological modifications in face of failures, according to the selected routing mechanism and pre-determined time synchronized message scheduling.

The security administration of ISA100 Wireless is optional and can be disactivated. The disactivation can lead to increased flexibility, improve the network effectiveness and increase the network lifetime. As mentioned earlier, the security manager implements the security design which depends on the adopted security policy. The security options typically range from (i) nonsecured networks (which are not recommended), to (ii) symmetrically secured networks, and (iii) assymetrically secured networks. The security administration of ISA100 Wireless is implemented at the link and transport layers [22]. In particular, the data are authenticated at link layer, while the data payload is encrypted using the Advanced Encryption Standard algorithm. ISA100 Wireless can also protect and secure the transport and payload header, at the transport layer.

B. CRITICAL CONTROL APPLICATIONS

ISA100 Wireless is particularly useful for addressing critical control applications through the implementation of Internet-oriented wireless networked control systems. In this network paradigm, sensor motes coupled with industrial physical plants obtain and propagate their data to the system manager over wireless channels. Then, the system managers apply different control commands based on these acquired data, which are then propagated to the actuators so as to adapt the behavior of the physical plant. The technical challenges associated with wireless industrial network design and implementation for critical control applications and the definition of related novel approaches, optimizations, algorithms, and protocols have been presented thoroughly in [32]–[34], and [35]. Based on the findings of those articles, we briefly discuss selected identified challenges and we outline the feasibility of addressing them with ISA100 Wireless.

- *Communication optimization*. The effective configuration of medium access control mechanisms in Internet-oriented wireless networked control systems is not trivial for critical control applications, as mentioned in [32]. The overall performance of such systems significantly depends on the dynamics of the industrial environment. For example, random MAC mechanisms are suitable for the cases where a large number of less dynamic devices are the core component of the wireless network. In this case, due to the high number of control loops, a scheduled MAC mechanism might lead to significant delays between the an event of interest and the transmission of the related information in its assigned slot. However, most time slots are underutilized, due to the fact that the traffic is lower in less dynamic networks. On the contrary, a scheduled MAC mechanism performs well in the case of more dynamic networks. Contention-based random access usually lowers the reliability and latency metrics in the case of dynamic networks with high amounts of traffic. In the case of random access approaches with high packet losses, the event-triggered control may further augment the traffic, which may eventually lead to instability situations. As [32] notes, such challenges can be technically addressed by optimizing the wireless communication aspects of ISA100 Wireless. Details on communication optimization aspects of ISA100 Wireless are presented in section IV-A.
- *Routing mechanisms*. The deployment of Internet-oriented wireless networked control systems is associated with several limitations in the network routing domain. For example, as mentioned in [34], the network nodes are subject to power drainage and failure and can potentially become unavailable. Also, the wireless communication channels can introduce delays

and unreliability' in the data propagation between the network nodes and, therefore, limit the application scalability. Consequently, according to [32], the routing mechanisms play an extremely important role in achieving high reliability and end-to-end delay guarantees, together with energy efficiency and robustness in large scale networked control systems. Various routing mechanisms have been proposed to achieve energy efficiency for traditional environments. However, the harsher and noisier industrial environments, necessitate routing mechanisms which additionally provide reliable transmissions. Details on the routing mechanism aspects of ISA100 Wireless are presented in section IV-B.

- *Real-time control*. It is usually desirable to be able to support multiple control loops in a same wireless industrial network, so as to reduce the costs and increase the flexibility. As mentioned in [33], the reliability and control metrics of such networks heavily rely on the effectiveness of the real-time wireless communication. Consequently, feedback control loops in a networked control system place strict constraints on reliability and real-time guarantees in wireless communication in order to prevent operational failures and accidents. For instance, in oil refinery deployments, the of oil tanks' spilling must be avoided by monitoring the oil level in real-time. However, some industrial plants consist of harsh environmental spaces for wireless communication due to unpredictable channel behaviors, limited bandwidth, multipath fading, physical obstacles and interference from nearby wireless devices. With the adoption of industrial wireless standards such as ISA100 Wireless, process monitoring and control functionalities have become able to achieve reliability and real-time wireless communication via spatial and spectrum diversity. Details on real-time control aspects of ISA100 Wireless are presented in section IV-C.
- *Energy management*. The management of the available energy supplies in the network can be performed in two ways, as mentioned in [35]: by targeting a low consumption or an efficient consumption. Regarding low consumption, the network nodes are usually fed by batteries and they are designed to be energy efficient in order to achieve longer network lifetimes. Regarding efficient consumption, in order to augment the energy efficiency of the wireless network, the energy consumption over the network needs to be balanced. Energy-aware management solutions and routing protocols are fundamental for energy balance and, consequently, increase the network lifetime. Details on the energy management aspects of ISA100 Wireless are presented in section IV-D.
- *Security administration*. Wireless networks are more prone to attacks in comparison with wired networks, in which the attacker needs to be physically connected to the network. Similarly, the typical wired security solutions do not immediately meet the requirements of the wireless networks security. As mentioned in [35], authenticity, integrity and confidentiality are significant target objectives. The significance of those objectives depends on the industrial application requirements. Examples of attacks and threats in wireless networks are node tampering, node control, denial of service and radio interference. A basic design objective is to implement an effective security administration, taking into account the weak abilities of the constrained hardware which is usually used and the required energy efficiency. Security administration is a fundamental cornerstone of the major industrial standards and in many cases is handled with equal significance in comparison with other requirements. A dedicated security manager is used in ISA100 Wireless for security services. Details on the security administration aspects of ISA100 Wireless are presented in section IV-E.

C. COMPARISON WITH WirelessHART (AND OTHER INDUSTRIAL WIRELESS stANDards)

ISA100 Wireless shares architectural characteristics with other industrial wireless standards, most notably with WirelessHART. In fact, and ISA100 Wireless have been described as competitors in the quest of becoming the de facto global standardized solution for wireless communication in industrial automated environments. In this section, we firstly describe some fundamental similarities and differences between the two standards, and then we report the state of the art regarding the comparisons that have been performed of the two standards. Finally, we also report the comparisons that have been performed regarding additional standards as well.

1) SIMILARITIES AND DIFFERENCES

ISA100 Wireless presents many systemic similarities with WirelessHART. For example, the choice of 2.4GHz frequency as communicational base, the adoption of synced TDMA access, as well as the fundamental concept of channel hopping are indicative resemblances of the two standards. In WirelessHART, the time slot size is set at 10ms, while in ISA100 Wireless it is variable and fixed to a specific value by the system manager when a node enters the network. Furthermore, to better address coexistence and interference aspects, both WirelessHART and ISA100 Wireless apply some spectrum-management approaches. Another common point is that both standards can apply configurable administration to ensure the security of the network, relying on a security manager for the generation and circulation of the security keys and the authentication of new nodes.

ISA100 Wireless also presents numerous technical similarities with WirelessHART. A complete introduction to the two protocols' diverse characteristics is given in [28]. The most important differences are extracted as follows. A first fundamental difference is that in WirelessHART, all network devices and adapters are defined as routers able to forward data to and from other network nodes, enabling a mesh

topology. Furthermore, all nodes are able to provision other nodes to enter the network. However, in ISA100 Wireless, the field device role is differentiated from the router role. This renders ISA100 Wireless field devices to be set as either end nodes with no routing ability or router nodes with routing ability. Consequently, an ISA100 Wireless deployment can form a star, star-mesh, or mesh network topology, depending on the roles of the network nodes. Furthermore, differently from WirelessHART though, the ISA100 Wireless network and transport layers make seamless use of 6LoWPAN, which allows the use of IPv6 (Internet) compatibility [19], making it suitable for the industrial Internet and the interconnected industries vision. Another difference resides in the application layer. WirelessHART inherits its application layer from the wired HART application layer, which includes the commands, responses, data types, and status reporting provided by the HART field communication standard. On the contrary, ISA100 Wireless application layer defines SW objects to model real world objects.

2) WORKS ON COMPARISONS WITH WirelessHART

Due to the increased resemblance of the two standards, there have been quite a few works presenting various aspects of comparative examination between ISA100 Wireless and WirelessHART.

In [36], the authors address and compare the main features of ISA100 Wireless and WirelessHART. They confront the two standards in the context of the Internet of Things within the vision of Industry 4.0. The analysis demonstrates that the two standards share a significant amount of similarities and that, in various industrial use cases, they perform in a complementary way. Some indications of successful co-existence are also provided. ISA100 Wireless though, is shown to have various functionalities which render it more adjustable to industrial applications. Specifically, (a) the support of IPv6 (Internet) interconnectivity, (b) the object-oriented and more modular application layer, and (c) the increased flexibility in multiple layers (time scheduling, cast schemes, device assignments).

The main contribution of [28] is the theoretical (systematic and technical) confrontation of ISA100 Wireless and WirelessHART. The authors note that although the two standards present some diversity, most of the basic characteristics of the fundamental wireless communication are similar, and that both standards can operate in harsh industrial environments and achieve reliable and robust performance.

[21] provides a review of popular wireless technologies usually used for control and monitoring use cases, including ISA100 Wireless and WirelessHART. It presents the advantages and the disadvantages of each standard and investigates the extent to which each standard can satisfy the strict industrial control and monitoring requirements. Furthermore, it reviews the solutions proposed by the research community, focusing in methods which apply to critical use cases with real-time and reliability industrial requirements. The paper also lays down specific important open problems based on the physical layer and the challenges that have yet to be resolved so as to permit the successful utilization of the standards in industrial control and monitoring applications.

3) WORKS ON COMPARISONS WITH WirelessHART AND OTHER STANDARDS

[12] presents another, wider confrontation, among ISA100 Wireless, ZigBee, WirelessHART, and WIA-PA, the design and architecture of which are comparatively investigated. The authors try to show the distinct characteristics of the standards, also justifying several design choices. They also present the resemblances and the diversities of the examined standards, as well as a suitability examination of each standard with respect to meeting the requirements of Industry 4.0.

In [37], ZigBee, WirelessHART and ISA100 Wireless are introduced as typical industrial wireless standards, and activities of international standardization and regional radio regulations are shown. Also in [20] the authors review 6LoWPAN, Zigbee, WirelessHART, ISA100 Wireless and OCARI. All those standards assume the same physical layer technology, but bring in significant architectural diversity in the higher layers. The paper tries to identify the most suitable sensor networking standard to reliable communication for electrical substation deployments in the presence of impulsive noise.

In [24], the authors select WirelessHART, ISA100 Wireless, as well as ZigBee and 802.15.4e MAC, and the WISA standard which employs IEEE 802.15.1. Then, they identify several quality-of-service industrial requirements, mainly based on reliability and efficient real-time management, and evaluate their performance so as to understand to which extent the requirements can be met. Their analysis surprisingly shows that those standards are not yet capable of meeting to the maximum extent the strict industrial real-time requirements. The authors also make reference to some security considerations of the aforementioned standards and they present potential attack schemes that would be able to harm the normal industrial network function. They conclude that the ISA100 Wireless is efficient against most of the presented threats, excluding: long-term jamming targeting all available frequencies, connection requests flooding and multiple collision attacks.

In [38] and [39], the authors study and conduct an evaluation of ISA100 Wireless, Zigbee and Wireless HART via Castalia on OMNeT++ simulator, and conclude that ISA100 Wireless outperforms WIrelessHART and Zigbee. This is (according to the analysis of the paper) due to the fact that ISA100 Wireless takes advantage of CSMA/CA with OQPSK, which makes its physical layer more effective. Also, the direct Internet compatibility helps ISA100 Wireless to interface with legacy standards and also helps to exchange data with different standards without necessitating complex routing gateway management.

[40] reviews the constraints of related standards process automation, supported short-range wireless technologies, as well as associated pros and cons. Particular focus is placed on ISA100 Wireless, WirelessHART and ZigBee.

TABLE 3. Notable differences among notable existing wireless standards (information extracted from [12]).

	ISA100 Wireless	WirelessHART	ZigBee	WIA-PA
resource allocation	central	central	combined	combined
P2P networking	✓	✓	✓	limited
portable/handheld	✓ (under conditions)	✓	✓ (under conditions)	×

A set of extracted features regarding existing techniques of selected industrial wireless standards, based on the analysis provided in [12], is presented in table 3.

Time slot administration and channel allocation are important design choices in communication resource allocation, in all standards. The approach for achieving this allocation can be central (through a system manager), distributed (at a local, node level), or combined (a selection between the previous two options). ISA100 Wireless and WirelessHART do not define how to implement the allocation of the network resources. By default, they use centralized resource allocation, in which the system manager uses information on topological characteristics and communication requirements, and requests from network devices and applications to come up with a schedule. The ZigBee resource allocation can be characterized as both centralized and distributed. The same holds for WIA-PA, in which the cluster heads assist the decentralization process.

P2P networking can be implemented in ISA100 Wireless, in the case that the network nodes are defined as routing devices. Also in ZigBee, although P2P networking is limited. In WirelessHART, the ability of all devices to act as a routers means that the system manager can initiate P2P networking between any devices. However, in the case of WIA-PA, the unique topological outline comprised of mesh and star subnetworks, lowers its P2P networking ability only within network clusters.

In many industrial use cases, handheld and portable user devices communicate with robotic elements and industrial equipment. ZigBee is not exclusively targeting demanding industrial applications, so it does not take into account this particular requirement. The rest of the standards though support the utilization and inclusion of handheld devices, rendering them able to be connected to the gateway or to a network node with routing capabilities.

4) PRACTICAL CHALLENGES AGAINST WirelessHART

As noted in [28], although both ISA100 Wireless and WirelessHART define some security administration methods to ensure the integrity of the deployment, some possible security weaknesses can occur in the ISA100 Wireless case. For WirelessHART, all security features are obligatory, while in ISA100 Wireless, numerous security features are defined as optional. Taking into account that security configuration necessitates additional processor memory, time and power, the introduction of obligatory security functions, like in WirelessHART, turns even the devices that do not need them into highly power hungry units and therefore reduces the network lifetime. However, the additional flexibility of the optional security functions of ISA100 Wireless can potentially pose a security threat for the standard itself and a barrier when it comes to interoperability.

This inherent flexibility of ISA100 Wireless can lead to further technical challenges regarding implementation complexity and interoperability. As noted in [36], from the standpoint of implementation, WirelessHART is quite simple, with a small number of configuration options and parameters. ISA100 Wireless, however, is a complex standard with numerous configuration options and optional parameters. The strict approach of WirelessHART makes sure that all nodes will behave similarly. This results though in a lack of flexibility to configure the behavior of the network according to specialized application needs. In ISA100 Wireless, the rich variety of available optional parameters provides greater flexibility for adapting to various application needs. On the other hand, this ability might lead to interoperability problems, due to the fact that different industrial actors might want to implement different features of ISA100 Wireless.

5) CONVERGENCE EFFORTS

The ISA100.12 subcommittee was created for providing system designers with a way to perform the convergence and end-users with educational materials which promote for successful deployments of both WirelessHART and ISA100 Wireless networks in industrial spaces. The design of a convergence specification to converge WirelessHART and ISA100 Wireless was included in the subcommittee's activities. The objectives of the ISA100.12 Convergence Subcommittee included a specification of techniques so that end-users would achieve high interoperability between WirelessHART and ISA100 Wireless networks that are deployed in the same industrial space, a comparison that would outline the differences between ISA100 Wireless and WirelessHART, and an ISA recommended practice, which would present solutions for a single wireless node to be placed and configured to run either ISA100 Wireless or WirelessHART.

The ISA100.12 subcommittee dropped its activities prior to defining a convergence approach for WirelessHART standard with the ISA100 Wireless standard. The subcommittee had drafted a request for proposals, requesting from third parties to propose a technical approach for creating a related specification. The fundamental technological incompatibilities preventing interoperability between WirelessHART and ISA100 Wireless were time synchronization, slot time, meshing methods, network addressing, and transport layer. One of the early results of the ISA100.12 meetings was a recommendation by a small group of end users that suppliers could ship products which would be configured by the supplier at the factory, or later by the end user, to operate on either WirelessHART or ISA 100 Wireless. This process was

TABLE 4. Communication optimization for ISA100 Wireless.

Article	Issue addressed	Method used	Results
[41]	channel quality and communication overhead variations	lightweight, adaptive and cooperative channel hopping	reduced channel hopping complexity and communication, increased anti-interference
[42]	reliability	adaptive channel diversity	65% reduced system delay under interference
[43], [44]			10^{-4} packet error rate is achieved with 0.85-1.30s delay,
[45]	IEEE 802.11b interference	analytical model for coexistence	acceptable packet error rate and satisfaction of delay requirements (significant channel interference)
[46]	performance of TDMA and CSMA/CA, such as maximum backoff exponent, duration of timeslot, period of superframe	MAC and physical layer simulation model	maximum throughput 35%
[47]	evaluation of the priority CSMA/CA	simulation model	increased bandwidth utilization and reduced access queueing delay

called dual-boot system, but it was not worth until users demanded it. Finally, there was no proposal that could solve the core problem: the creation of a technical approach that could include both WirelessHART and ISA100 Wireless and provide backward compatibility with the devices adopting both standards. The incompatibilities between the two standards consequently stayed unsolved, and the subcommittee dropped its activities.

IV. IMPROVEMENTS OF ISA100 WIRELESS CORE MECHANISMS

This section presents the core improvements on top of or in ISA100 Wireless that have been presented in the literature so far. We grouped those improvements in five fundamental categories; communication optimization, routing mechanisms, real-time control, energy management and security administration. For each group, we present the identified works of interest and an accompanying table with selected, extracted, interesting characteristics and observations. Also, for each group, we have identified selected research challenges which are presented in section VI.

A. COMMUNICATION OPTIMIZATION

The first group of works of our survey focuses on communication optimization for ISA100 Wireless. Those works are focusing on the lower layers of the standard and are exploiting the channel hopping and framing mechanisms so as to either investigate or improve its performance. Interference is in some cases considered, either in the implementation, or as a side effect. The details are depicted in Table 4. The main shortcoming of those works is that frequency hopping increases algorithmic complexity as well, and introduces additional overhead in the stack implementation.

1) CHANNEL HOPPING AND DIVERSITY

In [41], the authors point out that channel hopping in ISA100 Wireless is focusing on five characteristic hopping methods and does not take into consideration the online variations of channel quality and the communication extent and overhead. Therefore, they propose a lightweight channel hopping method for small-scale ISA100 Wireless networks. The method is cooperative and adaptive and selects a node among all available nodes while balancing their energy consumption, and periodically checks the consumed energy by skimming through all the channels so as to come up a channel list. The method inserts the related information in the payload field of the frame, a trick that can greatly reduce the communication overhead. Finally, the authors demonstrate that the introduced method can decrease the channel hopping communication overhead and complexity, and improve the standard hopping patterns as well as the interference management.

In [42], the authors present an adaptive channel diversity method for ISA100 Wireless enabled industrial monitoring. They use measured data in order to compute reliability metrics and improve it by selecting in real-time more robust channels. Then, in the performance evaluation part, they demonstrate that, for star topologies, their approach is able to reduce the data access delay by about 65% under wireless local area interference. Consequently, their approach can be convenient for calculating communication link quality in wireless radio use cases and for managing interference from additional existing devices in the space.

Another adaptive channel diversity method, which is again targeting reliability and delay metrics, is introduced in [43] and [44]. Here, the authors find the optimal channels based on the amount of online radio interference. In the performance evaluation part (which was conducted on a real testbed, again

TABLE 5. Routing mechanisms for ISA100 Wireless.

Article	Routing mechanism	Improvement	End-to-end delay
[48]	path throughput estimation	enhanced throughput	✓
[49]	graph generation considering schedule of time slot schedule in superframe	decreased round-trip delays	✓
[50], [51]	estimation of next hop residual energy and packet reception rate, integer linear programming	enhanced network lifetime	✓
[52]	co-existent CAN-ISA100 Wireless management	decreased delay	✓
[53]	finite-Markov model	reliability prediction	
[54]	spatial diversity by multiple backbone routers	redundancy	
[55]	cluster based route stored graph	flexible graph routing, graph generation efficiency without a system manager	

star topology but also multi-hop topology), a 10^4 packet error rate is achieved within very low delay. The authors validate their findings with additional simulations with stochastic variables.

2) HOLISTIC MODELING AND SIMULATION

Another work on wireless LAN interference management and coexistence is presented in [45]. The authors target at modeling the coexistence between ISA100 Wireless and IEEE 802.11b and at calculating the packet error rate and average end-to-end delay. They demonstrate that ISA100 Wireless performs well with respect to the packet error rate and satisfies the industrial delay requirements, especially under increased channel interference.

In [46], the authors evaluate the performance of the CSMA/CA and TDMA functions of ISA100 Wireless via accurate simulations of the physical and MAC layers. They variate significantly the network parameters in order to achieve a comprehensive evaluation of the maximum backoff exponent, the superframe period and the timeslot duration. The authors evaluate the throughput, delay, and power efficiency as the main network parameters and show that ISA100 Wireless significantly improves the throughput and that the parameter selection should be considered with care during the network design steps in order to achieve the optimal results.

In [47], the authors evaluate in simulations the ISA100 Wireless CSMA/CA, taking into account the influence of the backoff process and the priority to the chance of collision and successful slot utilization. They demonstrate that an increase in the numbers of priority classes can lead to higher network utilization and increased network lifetime.

B. ROUTING MECHANISMS

The second group of works of our survey focuses on routing mechanisms for ISA100 Wireless. Those works are focusing on the network layer of the standard and are typically suggesting new routing alternatives. End-to-end delay is considered in some cases, either in the design (minimization), or as an evaluation metric. The details are depicted in Table 5. The main shortcoming of this research line is the absence of a common routing framework with other standards, such as WirelessHART and the lack of large-scale open testbeds for efficient data routing solution testing.

1) DECREASING THE END-TO-END DELAY

The authors of [48] propose a routing mechanism that increases the throughput efficiency and decreases end-to-end delay in interference overloaded ISA100 Wireless-based (cognitive) networks. The proposed mechanism is tailored to clustered networks in which the sensed data are grouped before delivery to the recipient. The mechanism is using path-based maximum throughput estimation, and uses the most convenient paths in order to route the data. The authors demonstrate via simulations that the routing mechanism can enhance the throughput and decrease the end-to-end delay.

In [49], the authors note that the graph creation rule is not specified in ISA100 Wireless and that ISA recommends to implement custom graph creation approaches. Then, they propose a graph creation approach by taking into account the superframe slots. Their approach effectively propagates the data from the producer node to the consumer node while keeping the reliability levels high enough. The authors analyze the end-to-end and round-trip delays and they demonstrate that their approach can achieve lower delays when comparing to other state of the art approaches.

In [50] and [51] the authors introduce a routing mechanism that enhances the network lifetime and decreases the end-to-end delay. The proposed mechanism is shown effective in multi-hop topologies as well as in large-scale deployments. The generated data are able to be propagated via optimal paths, by computing the remaining node energy levels and the packet reception rates. Furthermore, the power requirements and the data access delay can be kept to a minimum level, as demonstrated with ILP techniques. The authors also demonstrate that their mechanism achieves significant energy efficiency and decreased data access delay.

TABLE 6. Real-time control for ISA100 Wireless.

Article	Real-time aspect	Method introduced	Metrics improved
[56]	network flow utilization	schedulability analysis	max utilization bound
[57], [58]	network management	dynamic resource reservation and management	higher network management efficiency
[59]	visual management	simulated reality topological distribution	online analysis, remote monitoring
[60]	network synchronization	self-stabilizing firefly synchronization	complete fault-tolerance, robustness against the interference, accuracy without any central control
[61]	network software design	modular application and system management design	successful control loop system building
[62]	message delivery hard requirements	message scheduling method on shared timeslots	real-time message delivery within deadlines
[63]	real-time delivery		throughput, end-to-end delay

In [52], the authors present a solution for deploying a multi-technology network consisting of the CAN and ISA100 Wireless standards. They use packet encapsulation and fragmentation so as to distribute the network data between the different technologies. They study via simulations the delay aspects of the multi-technology network. The evaluation results highlight that the ISA100 Wireless part becomes the network bottleneck and results in more than 95% of the overall end-to-end data access delay.

2) RELIABILITY, REDUNDANCY AND FLEXIBILITY

In [53], the authors focus on effectively predicting network reliability issues using a finite-Markov approach. Their approach can be used as a reliability preserving routing mechanism. In [54], the authors explore aspects of topological diversity under the presence of multiple backbone routers in ISA100 Wireless. They show how the backbone router activities and mesh routing can optimize the effects of topological diversity, and they highlight the superiority of the multi-backbone router redundancy via experimental demonstrations. In [55] the authors suggest that even if ISA100 Wireless introduces a straightforward and reliable graph routing mechanism, the graph routing is a static routing and consequently very inflexible. Therefore, they introduce an alternative cluster based graph storing method for routing, and show that it can address the drawbacks of the inflexible graph routing and that it can create the graphs efficiently in a distributed manner.

C. REAL-TIME CONTROL

The third group of works of our survey focuses on real-time control for ISA100 Wireless. Those works are focusing on the different layers of the standard and they cover a variety of real-time operations. The methods presented are diverse and target improvements of numerous metrics. The details are depicted in Table 6. The main shortcoming of this research line is the absence of a consolidated framework for real-time, local and distributed data management.

1) NETWORK ADMINISTRATION

In [56] the authors develop an analytical framework targeting network scheduling based on utilization metrics. This is an open research topic in the area of wireless sensor networks, applied also to ISA100 Wireless enabled systems. In their framework, they retrieve network paths of maximum utilization and label a path as schedulable if the overall utilization value does not surpass the maximum observed utilization value in the network. They demonstrate that the framework can achieve a very low runtime overhead, and a highly efficient utilization scheduling.

In [57] and [58], the authors design a distributed network administration method, which target at satisfying the industrial requirements in terms of real-time services, in the presence of low power wireless devices. This method dynamically reserves network resources on behalf of the routers and configures the wireless devices in localized star sub-topologies. The authors show that the method manages the entire network more efficiently than the pure ISA100 Wireless, maintaining at the same time low data access delay and increased network reliability.

In [59], the authors identify that visual administration of industrial wireless deployments necessitates both fast data management and increased interaction flexibility with the related GUI. However, they note that the state of the art visual administration systems are too simplistic and do not depict realistically enough the network spatial parameters. Examining the topological characteristics of ISA100 Wireless and WIA-PA standards, they propose a toolkit for depicting realistic spatial deployments of wireless networks. The toolkit offers a collection of universal and transparent functions which successfully implement visual remote monitoring and real-time administration of the industrial network.

2) SOFTWARE METHODOLOGIES

In [60], the authors present an insect-based real-time control approach focusing on synchronization for ISA100 Wireless networks. The approach is based on the synchronization

manner of South-East Asian male fireflies. The approach is self-stabilizing and gives the option to each node to return online after a central failure. In order to achieve this result, all network nodes are able to collaborate distributively targeting local synchronization. The simulation results show that the approach is highly fault tolerant during the returning online period, and comes with resistance on external interference.

In [61], the authors implement a modular SW methodology targeting the the application layer of ISA100 Wireless, and they give the hands-on details in order to implement it on the wireless HW. Then, they evaluate its performance and they show that the control loop system can be built successfully.

3) DATA SCHEDULING

In [62], the authors propose message allocation on dedicated time slots of ISA100 Wireless in order to address real time requirements, targeting both periodic and aperiodic real time data. They divide superframes in dedicated time slots which are mapped to the real time data and shared time slots which are mapped to non real time data and alarm data. Additionally, they classify network traffic in low and high and they adjust accordingly the schedulability of the data. The performance evaluation demonstrates that in this way, they are able to allocate real time data in superframes and multi-superframes. Therefore, the network consumers are receiving the real time data within the delay deadlines.

In [63], another data scheduling approach using timeslots sharing of ISA100 Wireless is proposed, in order to enhance real-time performance. In this case, consumers are grouped into distinct groups, and then take over the equivalent channels in the allocated time cycles by estimating a collision based stochastic threshold. The performance evaluation demonstrates that this approach significantly enhances the network throughput and the end-to-end data access delay.

D. ENERGY MANAGEMENT

The fourth group of works of our survey focuses on energy management for ISA100 Wireless. Those works are centered on different application areas of the standard. The details are depicted in Table 7. The main shortcomings of those works are the absence of theoretically proven tight upper bounds on network lifetime, and of a truly holistic network energy administration (based not only on individual devices).

TABLE 7. Energy management for ISA100 Wireless.

Article	Application area
[64]	petroleum refinery instrumentation network
[65]	energy-harvested wireless monitoring system
[66]	energy constrained I/O device requirements
[67]	
[68]	demand-response industrial smart grid

1) APPLICATION-SPECIFIC SOLUTIONS

Some works in this class focus on specific applications, and provide energy management solutions based on the ISA standard. A relevant example is [64], in which the authors present a petroleum refinery network configured with ISA100 Wireless. The authors make an interesting energy metric related statement, by highlighting that the most efficient energy management can be achieved when the definition of the network lifetime is based on the maximum rather than the average device energy consumption. The performance evaluation demonstrates that, in this way, it is possible to significantly increase the network lifetime compared to other related energy optimization approaches (also in the large scale).

2) ENERGY CONSTRAINED REQUIREMENTS

[65] focuses on novel energy harvesting for industrial networks, and [66] introduces a modification of ISA100 Wireless targeting the power efficiency requirements of ISA100-enabled devices. This modification applies distributed network administration by giving management role to the router nodes. It also introduces a router clustering technique with which nodes can select master routers. It is demonstrated that the modification additionally improves real time administration, data access delay and reliability.

The authors of [67] investigate the joining phase power efficiency. They propose a network joining approach trying to provide highly efficient energy harvesting. This approach achieves low joining times with respect to the original ISA100 Wireless joining approach. It also achieves reliable data propagation via using spatial diversity which again outperforms the ISA100 Wireless data publication through significant improvement in packet reception.

3) INDUSTRIAL SMART GRID

In [68], the authors design an industrial smart grid demand-response HW simulation tool. The tool focuses on energy consumption, control and monitoring, as well as wired and wireless industrial field networking. The authors use the tool in order to conduct an experimental evaluation of a use case and they highlight that through switching the field electricity demand from high to low demand intervals we can highly increase the grid performance.

E. SECURITY ADMINISTRATION

The fifth group of works of our survey focuses on security administration for ISA100 Wireless. In ISA100 Wireless, in general, the security manager generates, authenticates, stores and distributes the security keys targeting end-to-end security [19]. The approach presents commonalities with the security approach of WirelessHART. On the other hand, unlike WirelessHART, the security options are optional and can be disactivated, depending on the application requirements. For example, if the objective is flexibility and increased power efficiency, then, naturally security mechanisms can be (and usually are) disactivated. Therefore, ISA100 Wireless allows the network administrator to configure the standard parameters of the joining key. The details of these works are depicted in Table 8. The validation of the studies was performed either on certified devices, or on non

TABLE 8. Security services for ISA100 Wireless.

Article	Issue addressed	Method used	Validation
[69]	initial secret key distribution	public/symmetric key cryptography	-
[22]	threat prevention	rekeying, audit, distance-bounding	
[70]		nonce structure, message integrity code, symmetric key, modes of operations	non certified devices
[71]	anomalous events prevention	reputation-based early warning system	
[72]	security assurance	communication test and security function assessment	
[73]	security provisioning	provisioning verification	certified devices
[74]	key updates	optimal calculation of update time schedules	simulations

certified devices, or via simulations. The main shortcoming of this research line is the flexibility of the optional security features might be a security threat for ISA100 Wireless itself.

1) SECURITY REVIEWS

In [69], the authors provide a nice review of the actual ISA100 Wireless practice and the requirements for key distribution and they present a set of open challenges. In [22], the authors review the security characteristics of three industrial standards. First, they identify routing mechanism threats vulnerabilities. Then they analyze the inherent security weaknesses and intrusion points. Finally, they present some recommendations and countermeasures to guide industrial administrators to protect their deployments and to achieve high resilience in critical use cases.

2) VALIDATION WITH NON CERTIFIED DEVICES

[70] introduces a security approach which addresses security systems with symmetric key, and other related parameters, in order to protect the data propagation security for ISA100 Wireless. The authors emphasize the security threats in ISA100 Wireless networks and propose a holistic security framework. Then, they discuss different communications oriented security aspects, such as secure frame compositions and secure data propagation among the network nodes. Also, they present how to improve network security based on specific fundamental requirements, and they lay down an evaluation on ISA100 Wireless security testing.

In [71], the authors propose an ISA100 Wireless enabled early warning system for controlling the network performance. This is a clustering approach as well, in which the network nodes are allocated into clusters with a single node acting as cluster head. This node serves also as reputation administrator. The performance of this approach is experimentally validated in a smart grid use case with real devices.

In [72], the authors introduce a security assurance technology for ISA100 Wireless-enabled IoT devices, including communication security testing and and validation. They focus on implementation and deployment aspects of ISA100 Wireless and introduce specific parameters for security function assessment. They verify the suitability of the introduced security assurance by implementing the technology in a real testbed.

3) VALIDATION WITH CERTIFIED DEVICES

In [73], the authors focus on ISA100 Wireless to also examine security provisioning aspects. They provide an interesting verification using devices which implement the ISA100 Wireless standard as well as devices which are ISA Wireless certified.

4) VALIDATION VIA SIMULATIONS

In [74], the authors focus on key update times and they introduce a related two-step scheduling algorithm which can identify cases where keys might be compromised, such as rates of data generation, security quantification, etc. Firstly, the algorithm computes the optimal key update time, and secondly, it plans the schedule of the key updates. The algorithm considers data propagations of each node at the initial phase, when it creates the schedule for the key updates. Following the evaluation results, the algorithm minimizes the unnecessary computations of updates and adapts to different data propagations by adjusting diverse parameters.

V. REAL INDUSTRIAL DEPLOYMENTS

A significant part of the literature is devoted to the design, deployment and testing of actual industrial ISA100 Wireless based networking equipment. The deployments range from small scale prototypes and testbeds to large scale networks in industrial plants. Also, the significant interest about related implementations is shown by the large number of countries in which there have been related deployments. The exact works, number of nodes, types of deployment, purpose and location are depicted in Table 9. We have identified four types of deployment applications, namely, smart grid, SW development, sensor networks, and networked aerospace applications. Naturally, the sensor network type gathers the most attention.

A. SMART GRID DEPLOYMENTS

In [75], the authors employ ISA100 Wireless and WirelessHART in order to develop a demand response

TABLE 9. Deployments of ISA100 Wireless.

Article	Type	Purpose	Location
[75]	smart grid	energy consumption monitoring	China
[76]	SW development	protocol conformance testing	
[77]		field instrument adjustment and configuration	Japan
[78]		wired device conversion to wireless ISA100-compliant	
[25]	sensor networks	refinery plant pressure monitoring	
[79]		radio measurements on dry riverbed, industrial plant, anechoic chamber	
[80]		scalability, data update time and reliability evaluation	
[81]		pipe rack safety monitoring	South Korea
[82]		gas detection in underground mines	South Africa
[83]		monitoring of gas control, generator shaft seal and stator cooling water systems	India
[84]		integration with WirelessHART, condition monitoring	Thailand
[85]		address assignment algorithm	China
[86]		coexistence interference analysis	
[87]		integration with Ethernet, multi-connection and communication evaluation	
[13]		delay analysis under WirelessHART and Wi-Fi interference	Norway
[88]		experimental verification of the simulated 802.15.4 layer	Saudi Arabia
[65]		energy-harvested vibration monitoring in automotive manufacturing and railway transport	Italy / UK
[89]		KPI evaluation in dualstandard network	Romania
[90]	networked aerospace applications	replace intra-satellite traditional UWB data communications	
[91]		UWB redundant and reliable network determinism	Czech Republic
[92]		uncertain 802.11g interference evaluation	USA

deployment. They evaluate the performance of the deployment by controlling the electrical loads using the standards and obtaining their energy consumption data centrally.

B. SW DEVELOPMENT

FieldMate is a SW targeting field instrument adjustment and configuration, adopting specialized SW languages, such as Electronic Device Description Language and tools, such as Field Device Tool and Device Type Manager. The principal targets of this SW are (a) support of a wide range of field instruments and communication models, including ISA100 Wireless. Yokogawa has developed a device Device Type Manager, the technical features and effectiveness of which is reported in [77]. In [76], the authors develop an ISA 100 Wireless protocol conformance testing software and they validate its functionality in the lab by using real devices. In [78], the authors develop ISA100 Wireless Gateway Device Type Managers for network adapters. This network adapter line supports both Modbus and HART. Since the Gateway Device Type Manager is using FDT (Field, Device, Tool) technology, it promotes the utilization of typical Device Type Managers without any alterations and renders the configuration of those devices from FDT Frame application available.

C. SENSOR NETWORKS

In [25], the authors present an actual use case of industrial wireless network deployment in a refinery plant, based on ISA100 Wireless technology. The objective of this use case is remote pressure and temperature monitoring using numerous measuring nodes of the deployment. The main contribution of the paper is the replacement of the traditional pressure and thermal gauges which require periodic manual monitoring with real-time remote pressure and temperature data collection utilizing ISA100 Wireless based sensors. The authors demonstrate that, through this approach, they can achieve very resilient wireless data collection with decreased reception errors. Therefore, they argue that ISA100 Wireless introduces important advantages, such as improved operation efficiency, limited human errors and continuous monitoring of the deployment.

[79] presents radio measurements that were collected from a dry riverbed deployment without obstacles, on an industrial plant with and without line of sight communication, as well as in an anechoic chamber.

In [80], the authors evaluate the performance of an ISA100 Wireless network with respect to scalability, reliability, and data update time. The network includes 500 wireless devices (transceivers). The network status has been observed so as to validate the stable connections of the devices over one year, including metrics such as packet error rates. The authors show important performance gains with respect to communication distance, data update rate, reliability, and routing flexibility.

In [81], the authors present an ISA100 Wireless deployment on an industrial pipe rack targeting safety monitoring. They evaluate the deployment's performance in large-scale

petrochemical plants. The data collected from the network nodes reveal that the network can monitor the structural stability of the pipe rack in real-time, and come up with risk management indications emerging from the actual measurements.

In [82], the authors demonstrate, in South Africa, a network tailored at gas sensing in underground platinum mines. They target at exploring the utilization of ISA100 Wireless enabled detectors in underground mines. The detector's accuracy and communication performance (under multiple frequencies) has been demonstrated via an extensive experimental evaluation, highlighting that it is ideal for difficult deployments in such harsh terrains.

Another real-device implementation is presented in [83], where the authors try to boost end user involvement and trust in industrial standards, via the implementation of wireless networks and testbeds. They manage to achieve this objective by demonstrating high instrumental reliability, network resilience in presence of obstacles, as well as interference management, and extended lifetime.

[84] introduces an integration method of ISA100 Wireless and WirelessHART devices in a condition monitoring deployment using Wonderware InTouch software. This multi-radio environment is designed to provide automatic data delivery so as to support the envisioned monitoring application. The real-time operation is achieved through centrally buffering and mapping the collected diagnostic data to Modbus and TCP registers.

[85] investigates topological aspects of ISA100 Wireless networks, and presents an address assignment scheme for efficient access to network devices. The scheme is based on a three-layer hierarchy, focusing on assigning routing addresses to nodes. The testing results show that the scheme achieves great scalability and consumes less time for network formation with respect to other alternatives. Concluding, the scheme satisfies the address assignment requirements while overcoming any orphan nodes issues.

In [86], the authors note that the extensive use of known industrial standards lead to interference problems, as most of them are operating on the overcrowded 2.4 GHz ISM frequency band. Hence, they explore the data success rate of ISA100 Wireless and WirelessHART on the data link layer when coexisting with other IEEE 802.15.4 and IEEE 802.11n networks. The authors setup a real wireless testbed consisting of ISA100 Wireless, WirelessHART, ZigBee and IEEE 802.11n devices. The main focus of investigation is just the performance of the ISA100 Wireless and WirelessHART parts though (the rest are used for providing sources of interference). The testbed operates in a harsh environment with metallic objects and other industrial equipment which is further boosting interference effects. The performance evaluation gives important insights regarding wireless interference and coexistence abilities of those diverse standards.

A novel approach for access to the gateways, focusing on the application layer of ISA100 Wireless is proposed in [87], which implements an interconnection between ISA100 Wireless and Ethernet. The network contains four components: a wireless interface component (ISA100 Wireless), a wired interface component (Ethernet), a data caching component and a protocol conversion component. Every component is assigned to diverse networking tasks, in order to achieve seamless communication and data distribution in the network. The performance evaluation demonstrates that the gateway behavior is stable and reliable and that it is able to achieve internal efficient data administration and real-time monitoring in the network.

[13] explores the ways of setting up a wireless control network over ISA100 Wireless. The authors evaluate experimentally the real-time performance of ISA Wireless with respect to multiple networking configurations. An interesting observation coming from the evaluation is that the data delivery delay between the data producer and the network controller remains high for specific applications even in the case that the sensor sampling is happening following sub-second rates. Also, the variability of delay remains high, even when the wireless links are stable. This observation leads us to the conclusion that this setting is not suitable for low jitter, deterministic delay industrial control applications.

Another interesting set of results is presented in [88], in which the authors confront ISA100 Wireless physical layer experimental and simulated results. The first ones are obtained by a real industrial deployment, while the second ones are produces from the equivalent parameterized simulations in Matlab environment. The confrontation mainly concerns RSSI and data delivery rates, and the observed performance differences are attributed to external environment factors that could not be simulated in Matlab, such as dust which adds noise to the radio channel, and high temperature which adds additional (thermal) noise.

[65] presents the results of two representative use cases - self-powered vibration wireless control and monitoring for sophisticated industrial spaces, and reliable Internet connectivity for channel-hopping time-synchronized wireless deployments. The approach followed tackles the related issues by implementing an industrial control and monitoring network of energy harvesting wireless sensors that collaboratively estimate upcoming machine faults and achieve a real-time failure prediction.

The focus of [89] is to investigate the KPIs of a dual-radio industrial deployment (joining times, data delivery rates and client/server response times), on mesh and star topologies. The authors are using the technology of a dual-radio gateway in order to build a wireless testbed which includes both ISA100 Wireless and WirelessHART in a unique HW unit. The performance evaluation demonstrates that a dual-radio approach is able to combine the pros of each technology into a complete, better performing network.

D. NETWORKED AEROSPACE APPLICATIONS

In [91], the authors demonstrate the suitability of ultra-wideband systems for deterministic and reliable networks in aerospace applications. Time division multiple

access implements the determinism and the system manager is administrating the resource allocation. The centralized network management and provides redundant and reliable of network operation.

Ultra-wideband for space applications is also mentioned in [90], where ISA100 Wireless over an ultra-wideband radio channel is used for implementing and validating a network of intra-satellite wireless sensing units. The validation was conducted on a testbed which includes camera sensors as well as a wireless gateway, and the performance results highlight the suitability of the interplay of ISA100 Wireless and ultra-wideband for achieving robust wireless communication in a spacecraft environment.

In [92], the authors present a rigorous analysis of the effects of 802.11g interference on ISA100 Wireless-based and ZigBee Pro-based networks in a representative analog crewed aerospace environment. They conclude that ISA100 Wireless is proven more reliable, especially in unreliable and not easily manageable (due to interference) environments, such as satellites or interplanetary probes, which necessitate robust spectrum administration and environmental determinism.

VI. FUTURE CHALLENGES

After having extensively surveyed the entire research literature regarding ISA100 Wireless, we have identified some emerging development trends and open issues in the field.

A. COMMUNICATION OPTIMIZATION

Frequency hopping offers significant advantages for wireless control and monitoring: it is an efficient approach to contain interference from external devices using the same frequency band, and offers a more robust alternative to address the shortcomings of multipath interference. According to [12], frequency hopping can minimize interference and increase security guarantees in congested links for various technologies and use cases. Unfortunately, frequency hopping increases algorithmic complexity as well, and introduces additional overhead in the stack implementation. ISA100 Wireless research activity can contribute to the design of simple yet effective frequency hopping techniques with low complexity and communication overhead.

Interference detection solutions are incorporating more and more intelligence and are becoming more popular. In ISA100 Wireless, various detection solutions have appeared from the physical layer to the MAC layer. As highlighted in [23], different solutions can be designed so as to address diverse detection requirements.

B. ROUTING MECHANISMS

According to [83], commercial products adopting ISA100 Wireless routing mechanisms are not able to directly route the data to commercial products aligned to WirelessHART. This issue leads to an emergent need of efficient interplay and careful industrial network planning and management, so as to achieve maximum compatibility. For example, as demonstrated by some works presented in this paper, such as [89], the introduction of generic dual-standard frameworks could promote a facilitation to the experimental research community.

The solution testing trend of ISA100 Wireless shows that researchers have preferred examination of data routing in actual networked deployments (section V) over detailed simulations. This can be partly attributed to the fact that there has not been developed any open, easily accessible, detailed network simulator of ISA100 Wireless. Such a development could offer a useful tool to the networking community for convenient, large-scale data routing testing, alleviating the burden of setting up actual industrial equipment. Additionally, it would significantly assist the reproductibility of the ISA100 Wireless related algorithmic, system and network design.

C. REAL-TIME CONTROL

As noted in [93], distributed, real-time data management and control is a crucial aspect of modern industrial deployments, especially when the industrial operator needs the sensitive production data to be contained just in the industrial space, and to not be shared with external third-party cloud service providers. Distributed management services could be another important improvement on top ISA100 Wireless, and could offer the necessary flexibility required to maintain the extent of data distributiveness as required by the use case requirements. This could be potentially implemented for ISA100 Wireless via using peer-to-peer industrial routing mechanisms [94], or distributed data caching techniques [95].

D. ENERGY MANAGEMENT

Network lifetime maximization is a crucial issue, especially in remote, large-scale, wireless deployments [96]. Currently, it appears that there is no theoretically proven tight upper bound on the lifetime of ISA100 Wireless deployments [31]. Nevertheless, an important related approach is provided in [64], where the authors experimentally showcase that optimizing the system operation could still significantly increase the network lifetime.

Large scale efficient energy management and low power consumption can be further boosted not only by individual device optimization, but also through holistic network administration. Traditional methods of network energy management can be tailored to improve ISA100 Wireless systems as well; ranging from energy efficient routing design [97], large scale wireless energy harvesting [98], wireless power alternatives [99], and others.

E. SECURITY ADMINISTRATION

In ISA100 Wireless, most of the security functions are optional. Taking into account that security configuration necessitates additional processor memory, time and power, the introduction of obligatory security functions, like in WirelessHART, turns even the devices that do not need them into highly power hungry units and therefore reduces the network

lifetime. However, the additional flexibility of the optional security functions of ISA100 Wireless can potentially pose a security threat for the standard itself and a barrier when it comes to interoperability. As noted in [100], the absence of design specifications and ambiguous security definitions prevent the practical implementation of the standard, due to the fact that the system designers are required to have a detailed knowledge of all the core guidelines. [28] explains that evidence from practical activities to implement a WirelessHART protocol stack showed that performing the AES computations in SW on embedded devices is too time consuming to meet the 10ms time-slot requirements of WirelessHART. To meet the said requirements, an idea would be to use an AES HW accelerator. This problem can be located in ISA100 Wireless deployments as well, especially in the case that a variable time-slot duration of 10ms or less is utilized.

REFERENCES

[1] M. Conti, S. K. Das, C. Bisdikian, M. Kumar, L. M. Ni, A. Passarella, G. Roussos, G. Tröster, G. Tsudik, and F. Zambonelli, "Looking ahead in pervasive computing: Challenges and opportunities in the era of cyber–physical convergence," *Pervas. Mobile Comput.*, vol. 8, no. 1, pp. 2–21, Feb. 2012. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1574119211001271

[2] Z. Li, X. Zhou, and Y. Qin, "A survey of mobile edge computing in the industrial Internet," in *Proc. 7th Int. Conf. Inf., Commun. Netw. (ICICN)*, Apr. 2019, pp. 94–98.

[3] P. Robison, M. Sengupta, and D. Rauch, "Intelligent energy industrial systems 4.0," *IT Prof.*, vol. 17, no. 3, pp. 17–24, May 2015.

[4] T. P. Raptis, A. Passarella, and M. Conti, "Energy efficient network path reconfiguration for industrial field data," *Comput. Commun.*, vol. 158, pp. 1–9, May 2020.

[5] V. Kotsiou, G. Z. Papadopoulos, D. Zorbas, P. Chatzimisios, and A. F. Theoleyre, "Blacklisting-based channel hopping approaches in low-power and lossy networks," *IEEE Commun. Mag.*, vol. 57, no. 2, pp. 48–53, Feb. 2019.

[6] S. Li, Q. Ni, Y. Sun, G. Min, and S. Al-Rubaye, "Energy-efficient resource allocation for industrial cyber-physical IoT systems in 5G era," *IEEE Trans. Ind. Informat.*, vol. 14, no. 6, pp. 2618–2628, Jun. 2018.

[7] M. Gidlund, G. P. Hancke, M. H. Eldefrawy, and J. Akerberg, "Guest editorial: Security, privacy, and trust for industrial Internet of Things," *IEEE Trans. Ind. Informat.*, vol. 16, no. 1, pp. 625–628, Jan. 2020.

[8] M. Lucas-Estañ, M. Sepulcre, T. Raptis, A. Passarella, and M. Conti, "Emerging trends in hybrid wireless communication and data management for the industry 4.0," *Electronics*, vol. 7, no. 12, p. 400, Dec. 2018, doi: 10.3390/electronics7120400.

[9] E. Molina, O. Lazaro, M. Sepulcre, J. Gozalvez, A. Passarella, T. P. Raptis, A. Ude, B. Nemec, M. Rooker, F. Kirstein, and E. Mooij, "The autoware framework and requirements for the cognitive digital automation," in *Collaboration a Data-Rich World*, L. M. Camarinha-Matos, H. Afsarmanesh, and R. Fornasiero, Eds. Cham, Switzerland: Springer, 2017, pp. 107–117.

[10] T. P. Raptis, A. Passarella, and M. Conti, "Data management in industry 4.0: State of the art and open challenges," *IEEE Access*, vol. 7, pp. 97052–97093, 2019.

[11] 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.

[12] Q. Wang and J. Jiang, "Comparative examination on architecture and protocol of industrial wireless sensor network standards," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 3, pp. 2197–2219, 3rd Quart., 2016.

[13] W. Ikram, N. Jansson, T. Harvei, N. Aakvaag, I. Halvorsen, S. Petersen, S. Carlsen, and N. F. Thornhill, "Wireless communication in process control loop: Requirements analysis, industry practices and experimental evaluation," in *Proc. IEEE Emerg. Technol. Factory Autom. (ETFA)*, Sep. 2014, pp. 1–8.

[14] M. Nixon, "A comparison of WirelessHART and ISA100.11a," Emerson Process Management, St. Louis, MN, USA, Tech. Rep., Sep. 2012.

[15] A. Nasrallah, A. S. Thyagaturu, Z. Alharbi, C. Wang, X. Shao, M. Reisslein, and H. ElBakoury, "Ultra-low latency (ULL) networks: The IEEE TSN and IETF DetNet standards and related 5G ULL research," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 1, pp. 88–145, 1st Quart., 2019.

[16] I. Parvez, A. Rahmati, I. Guvenc, A. I. Sarwat, and H. Dai, "A survey on low latency towards 5G: RAN, core network and caching solutions," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 4, pp. 3098–3130, 3rd Quart., 2018.

[17] Z. Li, M. A. Uusitalo, H. Shariatmadari, and B. Singh, "5G URLLC: Design challenges and system concepts," in *Proc. 15th Int. Symp. Wireless Commun. Syst. (ISWCS)*, Aug. 2018, pp. 1–6.

[18] J. Sachs, G. Wikstrom, T. Dudda, R. Baldemair, and K. Kittichokechai, "5G radio network design for ultra-reliable low-latency communication," *IEEE Netw.*, vol. 32, no. 2, pp. 24–31, Mar. 2018.

[19] M. Raza, N. Aslam, H. Le-Minh, S. Hussain, Y. Cao, and N. M. Khan, "A critical analysis of research potential, challenges, and future directives in industrial wireless sensor networks," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 1, pp. 39–95, 1st Quart., 2018.

[20] F. Labeau, A. Agarwal, and B. Agba, "Comparative study of wireless sensor network standards for application in electrical substations," in *Proc. Int. Conf. Comput., Commun. Secur. (ICCCS)*, Dec. 2015, pp. 1–5.

[21] P. Zand, S. Chatterjea, K. Das, and P. Havinga, "Wireless industrial monitoring and control networks: The journey so far and the road ahead," *J. Sensor Actuator Netw.*, vol. 1, no. 2, pp. 123–152, Aug. 2012. [Online]. Available: http://www:mdpi:com/2224-2708/1/2/123

[22] C. Alcaraz and J. Lopez, "A security analysis for wireless sensor mesh networks in highly critical systems," *IEEE Trans. Syst., Man, Cybern. C, Appl. Rev.*, vol. 40, no. 4, pp. 419–428, Jul. 2010.

[23] D. Yang, Y. Xu, and M. Gidlund, "Coexistence of IEEE802.15.4 based networks: A survey," in *Proc. 36th Annu. Conf. IEEE Ind. Electron. Soc.*, Nov. 2010, pp. 2107–2113.

[24] D. Christin, P. S. Mogre, and M. Hollick, "Survey on wireless sensor network technologies for industrial automation: The security and quality of service perspectives," *Future Internet*, vol. 2, no. 2, pp. 96–125, Apr. 2010. [Online]. Available: http://www.mdpi.com/1999-5903/2/2/96

[25] T. Hasegawa, H. Hayashi, T. Kitai, and H. Sasajima, "Industrial wireless standardization - scope and implementation of isa sp100 standard," in *Proc. SICE Annu. Conf.*, Sep. 2011, pp. 2059–2064.

[26] S. Staff. (2018). *ISA100 WCI Launches Certification Services*. [Online]. Available: https://www.fierceelectronics.com/components/isa100-wci-launches-certification-services

[27] (2011). *ANSI/ISA-100.11a-2011 Wireless Systems for Industrial Automation: Process Control and Related Applications*. [Online]. Available: https://www.isa.org/store/ansi/isa-10011a-2011-wireless-systems-for-industrial-automation-process-control-and-related-applications/118261

[28] S. Petersen and S. Carlsen, "WirelessHART versus ISA100.11a: The format war hits the factory floor," *IEEE Ind. Electron. Mag.*, vol. 5, no. 4, pp. 23–34, Dec. 2011.

[29] I. Howitt and J. A. Gutierrez, "Ieee 802.15.4 low rate - wireless personal area network coexistence issues," in *Proc. IEEE Wireless Commun. Netw.*, vol. 3, Mar. 2003, pp. 1481–1486.

[30] J. W. Hui and D. E. Culler, "IPv6 in low-power wireless networks," *Proc. IEEE*, vol. 98, no. 11, pp. 1865–1878, Nov. 2010.

[31] K. Al Agha, M.-H. Bertin, T. Dang, A. Guitton, P. Minet, T. Val, and J.-B. Viollet, "Which wireless technology for industrial wireless sensor networks? The development of OCARI technology," *IEEE Trans. Ind. Electron.*, vol. 56, no. 10, pp. 4266–4278, Oct. 2009.

[32] P. Park, S. Coleri Ergen, C. Fischione, C. Lu, and K. H. Johansson, "Wireless network design for control systems: A survey," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 2, pp. 978–1013, 2nd Quart., 2018.

[33] C. Lu, A. Saifullah, B. Li, M. Sha, H. Gonzalez, D. Gunatilaka, C. Wu, L. Nie, and Y. Chen, "Real-time wireless sensor-actuator networks for industrial cyber-physical systems," *Proc. IEEE*, vol. 104, no. 5, pp. 1013–1024, May 2016.

[34] A. W. Al-Dabbagh and T. Chen, "Design considerations for wireless networked control systems," *IEEE Trans. Ind. Electron.*, vol. 63, no. 9, pp. 5547–5557, Sep. 2016.

[35] A. A. Kumar S., K. Ovsthus, and L. M. Kristensen., "An industrial perspective on wireless sensor networks — A survey of requirements, protocols, and challenges," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 3, pp. 1391–1412, 3rd Quart., 2014.

[36] J. D. Adriano, E. C. D. Rosario, and J. J. P. C. Rodrigues, "Wireless sensor networks in industry 4.0: WirelessHART and ISA100.11a," in *Proc. 13th IEEE Int. Conf. Ind. Appl. (INDUSCON)*, Nov. 2018, pp. 924–929.

[37] H. Hayashi, M. Hasegawa, and D. emachi, "Wireless technology for process automation," in *Proc. ICCAS-SICE*, Aug. 2009, pp. 4591–4594.

[38] A. Al-Yami, W. Abu-Al-Saud, and F. Shahzad, "On industrial wireless sensor network (IWSN) and its simulation using castalia," in *Proc. UKSim-AMSS 18th Int. Conf. Comput. Modeling Simulation (UKSim)*, Apr. 2016, pp. 293–298.

[39] A. Al-Yami, W. Abu-Al-Saud, and F. Shahzad, "Simulation of industrial wireless sensor network (IWSN) protocols," in *Proc. IEEE Conf. Comput. Commun. Workshops (INFOCOM WKSHPS)*, Apr. 2016, pp. 527–533.

[40] W. Ikram and N. F. Thornhill, "Wireless communication in process automation: A survey of opportunities, requirements, concerns and challenges," in *Proc. UKACC Int. Conf. CONTROL*, 2010, pp. 1–6.

[41] Y. Li and W. Hu, "A light-weighted cooperative adaptive channel hopping mechanism for industrial wireless ISA100 network," in *Proc. IEEE Int. Conf. Commun. Problem-Solving*, Dec. 2014, pp. 384–387.

[42] M. Miyazaki, R. Fujiwara, K. Mizugaki, and M. Kokubo, "Adaptive channel diversity method based on ISA100.11a standard for wireless industrial monitoring," in *Proc. IEEE Radio Wireless Symp.*, Jan. 2012, pp. 131–134.

[43] Y. Serizawa, T. Yano, M. Miyazaki, K. Mizugaki, R. Fujiwara, and M. Kokubo, "Verification of interference avoidance effect with adaptive channel diversity method based on ISA100.11a standard," in *Proc. IEEE Radio Wireless Symp.*, Jan. 2013, pp. 361–363.

[44] Y. Serizawa, R. Fujiwara, T. Yano, and M. Miyazaki, "Reliable wireless communication technology of adaptive channel diversity (ACD) method based on ISA100.11a standard," *IEEE Trans. Ind. Electron.*, vol. 64, no. 1, pp. 624–632, Jan. 2017.

[45] F. P. Rezha and S. Young Shin, "Performance analysis of ISA100.11a under interference from an IEEE 802.11b wireless network," *IEEE Trans. Ind. Informat.*, vol. 10, no. 2, pp. 919–927, May 2014.

[46] F. P. Rezha and S. Young Shin, "Performance evaluation of ISA100.11A industrial wireless network," in *Proc. IET Int. Conf. Inf. Commun. Technol. (IETICT)*, 2013, pp. 587–592.

[47] N. Quoc Dinh, S.-W. Kim, and D.-S. Kim, "Performance evaluation of priority CSMA-CA mechanism on ISA100.11a wireless network," in *Proc. 5th Int. Conf. Comput. Sci. Converg. Inf. Technol.*, Nov. 2010, pp. 991–996.

[48] P. T. A. Quang and D.-S. Kim, "Throughput-Aware Routing for Industrial Sensor Networks: Application to ISA100.11a," *IEEE Trans. Ind. Informat.*, vol. 10, no. 1, pp. 351–363, Feb. 2014.

[49] Y. Chung, K.-h. Kim, and S.-w. Yoo, "Time slot schedule based minimum delay graph in TDMA supported wireless industrial system," in *Proc. Int. Conf. Comput. Inf. Syst. Ind. Manage. Appl. (CISIM)*, Oct. 2010, pp. 265–268.

[50] T.-L. Pham and D.-S. Kim, "Lossy link-aware routing algorithm for ISA100.11a wireless networks," in *Proc. 11th IEEE Int. Conf. Ind. Informat. (INDIN)*, Jul. 2013, pp. 624–629.

[51] T.-L. Pham and D.-S. Kim, "Routing protocol over lossy links for ISA100.11a industrial wireless networks," *Wireless Netw.*, vol. 20, no. 8, pp. 2359–2370, Nov. 2014, doi: 10.1007/s11276-014-0747-5.

[52] S. Y. Shin and F. P. Rezha, "Extending CAN protocol with ISA100.11a wireless network," in *Proc. Int. Conf. ICT Converg. (ICTC)*, Oct. 2012, pp. 472–476.

[53] Q. Wang and P. Wang, "A finite-state Markov model for reliability evaluation of industrial wireless network," in *Proc. Int. Conf. Comput. Intell. Softw. Eng.*, Sep. 2010, pp. 1–4.

[54] Y. Ishii, "Exploiting backbone routing redundancy in industrial wireless systems," *IEEE Trans. Ind. Electron.*, vol. 56, no. 10, pp. 4288–4295, Oct. 2009.

[55] Y. Chung, K.-H. Kim, and S. W. Yoo, "Instant graph routing: Lightweight graph generation scheme," in *Proc. 5th Int. Conf. Ubiquitous Inf. Manage. Commun.*, New York, NY, USA, 2011, pp. 1–5, doi: 10.1145/1968613.1968702.

[56] V. P. Modekurthy, D. Ismail, M. Rahman, and A. Saifullah, "A utilization-based approach for schedulability analysis in wireless control systems," in *Proc. IEEE Int. Conf. Ind. Internet (ICII)*, Oct. 2018, pp. 49–58.

[57] P. Zand, K. Das, E. Mathews, and P. Havinga, "D-MHR: A distributed management scheme for hybrid networks to provide real-time industrial wireless automation," in *Proc. IEEE Int. Symp. Wireless, Mobile Multimedia Netw.*, Jun. 2014, pp. 1–3.

[58] P. Zand, K. Das, E. Mathews, and P. Havinga, "A distributed management scheme for supporting energy-harvested I/O devices," in *Proc. IEEE Emerg. Technol. Factory Autom. (ETFA)*, Sep. 2014, pp. 1–10.

[59] T. Wang and H. Zhao, "Design and implementation of simulated reality topological distribution for ISA100.11a networks and WIA-PA networks," in *Proc. Chin. Autom. Congr. (CAC)*, Nov. 2015, pp. 1187–1191.

[60] Y. Wei and D.-S. Kim, "A self-stabilized firefly synchronization method for the ISA100.11a network," in *Proc. Int. Conf. ICT Converg. (ICTC)*, Oct. 2013, pp. 881–886.

[61] W. Ping, Z. Haipeng, and L. Yong, "Design and implementation of industry wireless network control loop system," in *Proc. Int. Forum Inf. Technol. Appl.*, Jul. 2010, pp. 349–352.

[62] F. Dewanta, F. P. Rezha, and D.-S. Kim, "Message scheduling approach on dedicated time slot of ISA100.11a," in *Proc. Int. Conf. ICT Converg. (ICTC)*, Oct. 2012, pp. 466–471.

[63] T. Nhon and D.-S. Kim, "Traffic-aware message scheduling method for ISA100.11a," in *Proc. 11th IEEE Int. Conf. Ind. Informat. (INDIN)*, Jul. 2013, pp. 649–654.

[64] M. J. Herrmann and G. G. Messier, "Cross-layer lifetime optimization for practical industrial wireless networks: A petroleum refinery case study," *IEEE Trans. Ind. Informat.*, vol. 14, no. 8, pp. 3559–3566, Aug. 2018.

[65] K. Das, P. Zand, and P. Havinga, "Industrial wireless monitoring with energy-harvesting devices," *IEEE Internet Comput.*, vol. 21, no. 1, pp. 12–20, Jan. 2017.

[66] P. Zand, E. Mathews, K. Das, A. Dilo, and P. Havinga, "ISA100.11a: The ISA100.11a extension for supporting energy-harvested I/O devices," in *Proc. IEEE Int. Symp. Mobile Multimedia Netw.*, Jun. 2014, pp. 1–8.

[67] K. Das, E. Mathews, P. Zand, A. S. Ramirez, and P. Havinga, "Efficient I/O joining and reliable data publication in energy harvested ISA100.11a network," in *Proc. IEEE Int. Conf. Ind. Technol. (ICIT)*, Mar. 2015, pp. 2184–2191.

[68] Z. Luo, M. Alam, S. H. Hong, Y. Ding, A. Xu, and D. Kwon, "A hardware-in-the-loop simulator for demand response energy management in industrial facilities," in *Proc. Workshop Model. Simul. Cyber-Phys. Energy Syst. (MSCPES)*, Apr. 2015, pp. 1–6.

[69] A. Ray, J. Akerberg, M. Gidlund, and M. Bjorkman, "Initial key distribution for industrial wireless sensor networks," in *Proc. IEEE Int. Conf. Ind. Technol. (ICIT)*, Feb. 2013, pp. 1309–1314.

[70] X. Zhang, M. Wei, P. Wang, and Y. Kim, "Research and implementation of security mechanism in ISA100.11a networks," in *Proc. 9th Int. Conf. Electron. Meas. Instrum.*, Aug. 2009, pp. 4–716.

[71] C. Alcaraz, C. Fernandez-Gago, and J. Lopez, "An early warning system based on reputation for energy control systems," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 827–834, Dec. 2011.

[72] H. Kim, S. Kim, S. Kwon, W. Jo, and T. Shon, "A novel security framework for industrial iot based on isa 100.11a," in *Quality, Reliability, Security and Robustness in Heterogeneous Systems*, T. Q. Duong, N.-S. Vo, and V. C. Phan, Eds. Cham, Switzerland: Springer, 2019, pp. 61–72.

[73] S. Kwon, J. Jeong, and T. Shon, "Toward security enhanced provisioning in industrial IoT systems," *Sensors*, vol. 18, no. 12, p. 4372, Dec. 2018. [Online]. Available: http://www.mdpi.com/1424-8220/18/12/4372

[74] H. Jung, D. Yeop Hwang, W. Akram Baig, K. Hyung Kim, and S. Wha Yoo, "Optimizing time schedule of key updates in ISA100.11a," in *Proc. 4th Int. Conf. Ubiquitous Future Netw. (ICUFN)*, Jul. 2012, pp. 434–439.

[75] M. Alam, J. Kim, Y.-C. Li, S. H. Hong, X. Li, and A. Xu, "Implementation of wireless industrial networks for industrial smart grids," in *Proc. Int. Conf. Adv. Energy Convers. Technol. (ICAECT)*, Jan. 2014, pp. 83–87.

[76] H. Xie, N. Ren, and P. Wang, "Design and realization of object-oriented system for ISA100.11a protocol conformance testing," in *Proc. IEEE 3rd Int. Conf. Commun. Softw. Netw.*, May 2011, pp. 525–529.

[77] H. Fujii, "Dtm supporting a wide range of field instruments and field networks," in *2012 Proc. SICE Annu. Conf. (SICE)*, Aug. 2012, pp. 955–958.

[78] T. Sakurai and S. Yamamoto, "Gateway DTM for ISA100.11a wireless adapter supporting HART and modbus protocol," in *Proc. SICE Annu. Conf. (SICE)*, Sep. 2014, pp. 1138–1143.

[79] T. Hasegawa and M. Matsuzaki, "Reliable radio with ISA100 for wireless industrial automation," in *Proc. Future Instrum. Int. Workshop (FIIW) Proc.*, Nov. 2011, pp. 106–109.

[80] T. Hasegawa and S. Yamamoto, "Design and execution of a," plant wide isa100 wireless" network for optimization of complex process industries," in *2015 54th Annu. Conf. Soc. Instrum. Control Eng. Jpn. (SICE)*, Jul. 2015, pp. 158–163.

[81] J. Jung and B. Song, "The possibility of wireless sensor networks for industrial pipe rack safety monitoring," in *Proc. 47th Hawaii Int. Conf. Syst. Sci.*, Jan. 2014, pp. 5129–5134.
[82] A. M. Abu-Mahfouz, S. J. Isaac, C. P. Kruger, N. Aakvaag, and B. Fismen, "Wireless gas sensing in south african underground platinum mines," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Apr. 2014, pp. 3432–3437.
[83] K. B. Batra and S. Srivastava, "Wireless sensor network–performance evaluation in the field," in *Proc. 2nd Int. Conf. Power, Control Embedded Syst.*, Dec. 2012, pp. 1–8.
[84] A. Tanyakom, S. Pongswatd, A. Julsereewong, and A. Rerkratn, "Integration of WirelessHART and ISA100.11a field devices into condition monitoring system for starting IIoT implementation," in *Proc. 56th Annu. Conf. Soc. Instrum. Control Engineers Jpn. (SICE)*, Sep. 2017, pp. 1395–1400.
[85] T. Wang and H. Zhao, "A borrowed address assignment algorithm for ISA100.11a networks based on DAMM algorithm," in *Proc. Chin. Autom. Congr. (CAC)*, Nov. 2015, pp. 1182–1186.
[86] Y. Ding, S. H. Hong, R. Lu, J. Kim, Y. H. Lee, A. Xu, and L. Xiaobing, "Experimental investigation of the packet loss rate of wireless industrial networks in real industrial environments," in *Proc. IEEE Int. Conf. Inf. Autom.*, Aug. 2015, pp. 1048–1053.
[87] Z. Chen, X. Zhao, Z. Zhang, Z. Fan, C. Duan, S. Sang, X. Zheng, and L. Qin, "Software design and implementation of WSN access gateway based on ISA100.11a," in *Proc. IEEE Int. Conf. Commun. Problem-Solving*, Dec. 2014, pp. 299–302.
[88] A. Al-Yami, W. Abu-Al-Saud, and A. Zidouri, "Practical vs. Simulated results of ISA100 physical layer," in *Proc. 6th Int. Conf. Intell. Syst., Modeling Simulation*, Feb. 2015, pp. 226–230.
[89] E. Jecan, C. Pop, Z. Padrah, O. Ratiu, and E. Puschita, "A dual-standard solution for industrial wireless sensor network deployment: Experimental testbed and performance evaluation," in *Proc. 14th IEEE Int. Workshop Factory Commun. Syst. (WFCS)*, Jun. 2018, pp. 1–9.
[90] O. Ratiu, N. Panagiotopoulos, S. Vos, and E. Puschita, "Wireless transmission of sensor data over UWB in spacecraft payload networks," in *Proc. 6th IEEE Int. Conf. Wireless Space Extreme Environ. (WiSEE)*, Dec. 2018, pp. 131–136.
[91] P. Moravek and V. Stencel, "UWB network demonstrator for space applications," in *Proc. IEEE Int. Conf. Wireless Space Extreme Environ. (WiSEE)*, Oct. 2014, pp. 1–2.
[92] R. S. Wagner and R. J. Barton, "Performance comparison of wireless sensor network standard protocols in an aerospace environment: ISA100.11a and ZigBee pro," in *Proc. IEEE Aerosp. Conf.*, Mar. 2012, pp. 1–14.
[93] T. P. Raptis, A. Passarella, and M. Conti, "Distributed data access in industrial edge networks," *IEEE J. Sel. Areas Commun.*, vol. 38, no. 5, pp. 915–927, Feb. 2020.
[94] C.-M. Tang, Y. Zhang, and Y.-P. Wu, "The P2P-RPL routing protocol research and implementation in contiki operating system," in *Proc. 2nd Int. Conf. Instrum., Meas., Comput., Commun. Control*, Dec. 2012, pp. 1472–1475.
[95] T. Raptis, A. Passarella, and M. Conti, "Performance analysis of latency-aware data management in industrial IoT networks," *Sensors*, vol. 18, no. 8, p. 2611, Aug. 2018, doi: 10.3390/s18082611.
[96] T. P. Raptis, A. Passarella, and M. Conti, "Maximizing industrial IoT network lifetime under latency constraints through edge data distribution," in *Proc. IEEE Ind. Cyber-Physical Syst. (ICPS)*, May 2018, pp. 708–713.
[97] J. Vazifehdan, R. V. Prasad, and I. Niemegeers, "Energy-efficient reliable routing considering residual energy in wireless ad hoc networks," *IEEE Trans. Mobile Comput.*, vol. 13, no. 2, pp. 434–447, Feb. 2014.
[98] N. A. Bhatti, M. H. Alizai, A. A. Syed, and L. Mottola, "Energy harvesting and wireless transfer in sensor network applications: Concepts and experiences," *ACM Trans. Sensor Netw.*, vol. 12, no. 3, pp. 1–40, Aug. 2016, doi: 10.1145/2915918.
[99] I. Katsidimas, S. Nikoletseas, T. P. Raptis, and C. Raptopoulos, "An algorithmic study in the vector model for wireless power transfer maximization," *Pervas. Mobile Comput.*, vol. 42, pp. 108–123, Dec. 2017. [Online]. Available: http://www:sciencedirect:com/science/article/pii/S1574119217301803
[100] S. Raza, T. Voigt, A. Slabbert, and K. Landernas, "Design and implementation of a security manager for WirelessHART networks," in *Proc. IEEE 6th Int. Conf. Mobile Adhoc Sensor Syst.*, Oct. 2009, pp. 995–1004.

THEOFANIS P. RAPTIS received the Ph.D. degree from the University of Patras, Greece. He was an Associate Researcher with the Computer Technology Institute and Press Diophantus, Greece. He is currently a Research Scientist with the National Research Council, Italy. He has published in journals, conference proceedings, and books, more than 60 articles on industrial networks, wirelessly powered networks, Internet of Things testbeds, and platforms. He is also regularly involved in international IEEE and ACM sponsored conference and workshop organization committees, in the areas of networks, computing, and communications. He has been serving as an Associate Editor for the IEEE Access journal and a Guest Editor for *Computer Communications* (Elsevier) journal.

ANDREA PASSARELLA received the Ph.D. degree in 2005. He is currently a Research Director with the Institute for Informatics and Telematics (IIT), National Research Council, Italy (CNR). Prior to join IIT, he was with the Computer Laboratory, University of Cambridge, U.K. He is the coauthor of the book *Online Social Networks: Human Cognitive Constraints in Facebook and Twitter Personal Graphs* (Elsevier, 2015). He has published more than 160 articles on human-centric data management for self-organising networks, online and mobile social networks, opportunistic, and ad hoc and sensor networks. He received four best paper awards, including at IFIP Networking 2011 and IEEE WoWMoM 2013. He was the General Co-Chair for IEEE WoWMoM 2019 and the Workshops Co-Chair for IEEE INFOCOM 2019. He was the PC Co-Chair of IEEE WoWMoM 2011, the Workshops Co-Chair of ACM MobiHoc 2015, IEEE PerCom, and WoWMoM 2010, and the Co-Chair of several IEEE and ACM workshops. He is the Chair of the IFIP WG 6.3 Performance of Communication Systems. He is also the founding Associate EiC of the new Elsevier journal *Online Social Networks and Media* (OSNEM). He was a Guest Co-Editor of the several special issues/sections in ACM and Elsevier Journals and of the book *Multi-hop Ad hoc Networks: From Theory to Reality* (2007).

MARCO CONTI is currently a Research Director and a Scientific Counselor for information and communication technologies of the Italian National Research Council. He has published in journals and conference proceedings more than 400 scientific articles related to design, modeling, and experimentation of Internet architecture and protocols, pervasive systems, and social networks. He has published the books *Metropolitan Area Networks (MANs)* (1997), *Mobile Ad Hoc Networking* (2004), *Mobile Ad hoc Networking: The Cutting Edge Technologies* (2013) and *Online Social Networks: Human Cognitive Constraints in Facebook and Twitter Personal Graphs* (2015). He received several awards, including the Best Paper Award at IFIP TC6 Networking 2011, IEEE ISCC 2012, and IEEE WoWMoM 2013. He has served as a TPC Chair for several major conferences, such as IFIP Networking 2002, IEEE WoWMoM 2005, IEEE PerCom 2006, and ACM MobiHoc 2006. He was a General Chair (among many others) for IEEE WoWMoM 2006, IEEE MASS 2007, and IEEE PerCom 2010. He is the founder of successful conference and workshop series, such as IEEE AOC, ACM MobiOpp, and IFIP SustainIT. He is the founding Editor-in-Chief of *Online Social Networks and Media* journal, the Editor-in-Chief for special issues of *Pervasive and Mobile Computing* journal and, from several years, the Editor-in-Chief of *Computer Communications* journal, all published by Elsevier.