Industrial Internet of Things: Challenges, Opportunities, and Directions

Emiliano Sisinni, *Member, IEEE,* Abusayeed Saifullah, *Member, IEEE,* Song Han, *Member, IEEE* Ulf Jennehag, *Member, IEEE* and Mikael Gidlund, *Senior Member, IEEE*

***Abstract*—Internet of Things (IoT) is an emerging domain that promises ubiquitous connection to the Internet, turning common objects into connected devices. The IoT paradigm is changing the way people interact with things around them. It paves the way to creating pervasively connected infrastructures to support innovative services and promises better flexibility and efficiency. Such advantages are attractive not only for consumer applications, but also for the industrial domain. Over the last few years, we have been witnessing the IoT paradigm making its way into the industry marketplace with purposely designed solutions. In this paper, we clarify the concepts of IoT, Industrial IoT, and Industry 4.0. We highlight the opportunities brought in by this paradigm shift as well as the challenges for its realization. In particular, we focus on the challenges associated with the need of energy efficiency, real-time performance, coexistence, interoperability, and security and privacy. We also provide a systematic overview of the state-of-the-art research efforts and potential research directions to solve Industrial IoT challenges.**

***Index Terms*—Industrial Internet of Things (IIoT), Wireless Sensor Network (WSN), Real-time communication, Reliability, Security.**

I. Introduction

Internet of Things (IoT) is a computing concept describing ubiquitous connection to the Internet, turning common objects into connected devices. The key idea behind the IoT concept is to deploy billions or even trillions of smart objects capable to sense the surrounding environment, transmit and process acquired data, and then feedback to the environment. It is expected that by the year 2021 there will be around 28 billion connected devices [1]. Connecting unconventional objects to the Internet will improve the sustainability and safety of industries and society, and enable efficient interaction between the physical world and its digital counterpart, *i.e.* what is usually addressed as a Cyber-physical System (CPS). IoT is usually depicted as the disruptive technology for solving most of present-day society issues such as smart cities, intelligent transportation, pollution monitoring, connected healthcare, to name a few. As a subset of IoT (see Fig. 1), *Industrial IoT (IIoT)* covers the domains of machine-to-machine (M2M) and industrial communication technologies with automation applications. IIoT paves the way to better understanding of the manufacturing process, thereby enabling efficient and sustainable production.

Flexibility and scalability required by IoT communications are typically addressed using wireless links. In the past, wireless technologies in industrial applications were mostly based on ad hoc solutions, *e.g.* individually developed for connecting moving parts or hard-to-reach devices. Only recently, standards purposely designed for the industry (e.g., WirelessHART [2] and ISA100.11a [3]) were released. However, they face limitations in terms of scalability and coverage when very large areas need to be covered. While cellular technologies such as 3/4/5G technologies promise to connect massive devices over long distances, they require infrastructure support and licensed band [4]. IIoT applications typically require relatively small throughput per node and the capacity is not a main concern. Instead, the need of connecting a very large number of devices to the Internet at low cost, with limited hardware capabilities and energy resources (*e.g.* small batteries) make latency, energy efficiency, cost, reliability, and security/privacy more desired features [5].

Meeting the above mentioned requirements poses a number of key challenges on the evolution of IIoT. Addressing these challenges is critical in order to ensure a massive roll-out of IIoT technologies. In this paper, we clarify the concepts of IoT, IIoT, and the current trend of automation and data exchange in manufacturing technologies called *Industry 4.0*. We highlight the opportunities brought in by IIoT as well as the challenges for its realization. In particular, we focus on the challenges associated with the need of energy efficiency, real-time performance, coexistence, interoperability, and with the security and privacy issues. We also provide a systematic overview of the state-of-the-art research efforts and potential future research directions to address Industrial IoT challenges.

The rest of this paper is organized as follows. Section II compares IoT, IIoT, and Industry 4.0. Section III provides an overview of the recent activities on the definition of the IIoT architecture, protocol stack, as well as the standardization efforts. Section IV describes opportunities that IIoT will offer and challenges that have to be solved. Finally, we give some concluding remarks in Section V.

II. IoT, IIoT and Industry 4.0

IoT, IIoT and Industry 4.0 are closely related concepts but cannot be interchangeably used. In this section, we provide a rough classification of these terms. Regarding the IoT, several

Emiliano Sisinni is with the Department of Information Engineering, University of Brescia, 25123 Brescia, Italy e-mail: emiliano.sisinni@unibs.it

Abusayeed Saifullah is with the Department of Computer Science, Wayne State University, Detroit, USA e-mail: saifullah@wayne.edu

Song Han is with the Department of Computer Science and Engineering, University of Connecticut, Storrs, USA e-mail: song.han@engr.uconn.edu

Ulf Jennehag and Mikael Gidlund are with Department of Information Systems and Technology, Mid Sweden University, SE-851 70 Sundsvall, Sweden e-mail: firstname.lastname@miun.se

definitions exist, each one trying to capture one of its fundamental characteristics. It is often considered as a sort of web for the machines, highlighting the aim of allowing things to exchange data. However, application fields are so diverse that some requirements (especially those related to communication aspects) can be very different, depending on the intended goals and end-users, the underlying business models and the adopted technological solutions. What is usually addressed as IoT, could be better named as consumer IoT, as opposed to industrial IoT [6], [7].

Consumer IoT is human-centered; the "things" are smart consumer electronic devices interconnected with each other in order to improve human awareness of the surrounding environment, saving time and money. In general, consumer IoT communications can be classified as machine-to-user and in the form of client-server interactions.

On the other hand, in the industrial world we are assisting to the advent of the digital and smart manufacturing, which aim at integrating Operational Technology (OT) with Information Technology (IT) domains [8]. In very few words, the IIoT (the basic pillar of digital manufacturing), is about connecting all the industrial assets, including machines and control systems, with the information systems and the business processes. As a consequence, the large amount of data collected can feed analytics solutions and lead to optimal industrial operations. On the other hand, smart manufacturing obviously focuses on the manufacturing stage of (smart) products life-cycle, with the goal of quickly and dynamically respond to demand changes. Therefore, the IIoT affects all the industrial value chain and is a requirement for smart manufacturing.

As underlined in the following, communication in IIoT is machine oriented, and can range across a large variety of different market sectors and activities. The IIoT scenarios include legacy monitoring applications (e.g., process monitoring in production plants) and innovative approaches for self-organizing systems (e.g., autonomic industrial plant that requires little, if any, human intervention) [9].

While the most general communication requirements of IoT and IIoT are similar, *e.g.* support for the Internet ecosystem using low-cost, resource-constrained devices and network scalability, many communication requirements are specific to each domain and can be very different, *e.g.* Quality of Service (QoS) (in terms of determinism, latency, throughput, etc.), the availability and reliability, and the security and privacy. IoT focuses more on the design of new communication standards which can connect novel devices into the Internet ecosystem in a flexible and user-friendly way. By contrast, the current design of IIoT emphasizes on possible integration and interconnection of once isolated plants and working islands or even machineries, thus offering a more efficient production and new services [9]. For this reason, compared with IoT, IIoT can be considered more an evolution rather than a revolution. Table I gives a qualitative comparison of these technologies.

Regarding the connectivity and criticality, IoT is more flexible, allowing ad hoc and mobile network structures, and having less stringent timing and reliability requirements (except for medical applications). On the other hand, IIoT typically employs fixed and infrastructure-based network solutions that are well designed to match communication and coexistence needs. In IIoT, communications are in the form of machine-to-machine links that have to satisfy stringent requirements in terms of timeliness and reliability. Taking process automation as an example domain where process monitoring and control applications can be grouped into three sub-categories: monitoring/supervision, closed loop control, and interlocking and control. While monitoring and supervision applications are less sensitive to packet loss and jitter and can tolerate transmission delay at second level, closed loop control and interlocking and control applications require bounded delay at millisecond level (10-100ms) and a transmission reliability of 99.99% [5].

TABLE I
COMPARISON BETWEEN CONSUMER IOT AND INDUSTRIAL IOT

	Consumer IoT	Industrial IoT
Impact	Revolution	Evolution
Service Model	Human-centered	Machine-oriented
Current Status	New devices and standards	Existing devices and standards
Connectivity	Ad-Hoc (infrastructure is not tolerated; nodes can be mobile)	Structured (nodes are fixed; centralized network management)
Criticality	Not stringent (excluding medical applications)	Mission critical (timing, reliability, security, privacy)
Data Volume	Medium to High	High to Very High

Comparing the data volume, the generated data from IoT is heavily application dependent, while IIoT currently targets at analytics, e.g. for predictive maintenance and improved logistics. This implies that very large amount of data are exchanged in IIoT. For example, it is reported that the Rio Tinto mine generates up to 2.4TB of data per minute, according to Cisco Global Cloud Index.

The concept of *Industry 4.0* (where 4.0 represents the fourth industrial revolution) arises when the IoT paradigm is merged with the Cyber-Physical Systems (CPSs) idea [10]. Originally defined in Germany, the Industry 4.0 concept has gained a global visibility and it is nowadays universally adopted for addressing the use of Internet technologies to improve production efficiency by means of smart services in smart factories. CPSs extend real-world, physical objects by interconnecting them altogether and providing their digital descriptions. Such information, stored in models and data objects that can be updated in real time, represents a second identity of the object itself and constitutes a sort of "digital twin". Thanks to the dynamic nature of these digital twins, innovative services, that were not possible in the past, can be implemented across the whole product lifecycle, from inception to disposal of manufactured products. In summary, IIoT is a subset of IoT which is specific to industrial applications. The manufacturing phase of the product lifecycle is where the IoT and Industry 4.0 meet, originating to the IIoT. Figure 1 shows intersections of IoT, CPS, IIoT, and Industry 4.0.

As a concluding remark, it has to be highlighted that the IIoT paradigm is not intended for substituting traditional automation applications, but aims at increasing the knowledge

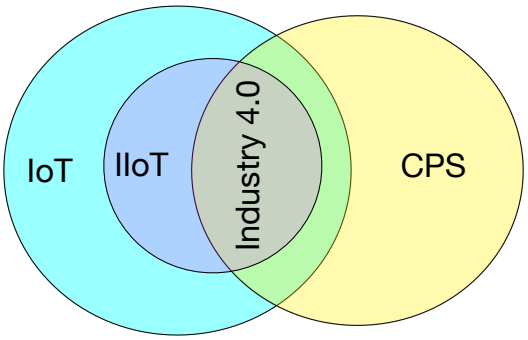

Fig. 1. IoT, CPS, IIoT, and Industry 4.0 in Venn Diagram.

about the physical system of interest. As a consequence, the IIoT (at least today) is not related to control applications at the field level, where bounded reaction time (i.e. determinism) must be ensured. On the contrary, as previously stated, IIoT applications including supervision, optimization, and prediction activities, are typically grouped into the so called Digital or Cloud Manufacturing (CM). The growing interest toward this topic is confirmed by the wide range of literature. A survey about CM is reported in [11]. In the past, the supervision activities were dominated by the man, but efficient machine to machine communications make human intervention superfluous and extend the operating range to geographical scale. For instance, the availability of reliable, short latency connections on such a large scale may increase the revenue [12]. The work in [13] highlights the importance of real-time, large-scale approach for equipment maintenance applications. An IIoT-based dynamic production logistics architecture is presented in [14] for real-time synchronization of internal and public production logistics resources. In [15], the optimization of production scheduling is based on IIoT decentralized energy prediction algorithms fed by the current state of the machines. As a concluding remark, the progressive reduction of latency and jitter of Internet-based connectivity will increase the range of possible applications, as reported in [16].

III. State of The Art

As IIoT interconnects a large number of components leveraging sensing, communication and data processing technologies, it is not possible to have a comprehensive description of all the recent advancements in such a diverse field. However, some foundational aspects can be highlighted, *i.e.* the architecture, the connectivity and the standardization.

A. The IIoT architecture

A *reference architecture* is a higher level of abstraction description that helps identify issues and challenges for different application scenarios. The design of a IIoT architecture needs to highlight extensibility, scalability, modularity, and interoperability among heterogeneous devices using different technologies. Several reference architecture frameworks originated in the past in different application contexts for both IoT and IIoT [17]. The typically adopted approach is a multi-layer description organized around the services offered at each level, depending on the selected technologies, business needs, and technical requirements. For instance, the International Telecommunication Union (ITU) supports an IoT architecture made of five layers: sensing, accessing, networking, middleware, and application layers. Jia et al. [18], Domingo [19], and Atzori et al. [20] suggested the identification of three major layers for IoT: perception layer (or sensing layer), network layer, and service layer (or application layer). Liu et al. [21] designed an IoT application infrastructure that contains the physical layer, transport layer, middleware layer, and applications layer. In [22] a four-layered architecture is derived from the perspective of offered functionalities, that includes the sensing layer, the networking layer, the service layer and the interface layer. The Reference Architectural Model Industrie 4.0 (RAMI 4.0) [23] focuses on next-generation industrial manufacturing systems; it identifies a 3-D model whose axes are the Life Cycle & Value Stream, related to products life cycle, and the Hierarchy Levels, related to the different component functionalities. The Hierarchy axis describes the IT representative and includes a communication layer.

Recently, the Industrial Internet Consortium released the "Reference Architecture" document [24]. In particular, it focuses on different viewpoints (formally business, usage, functional and implementation views) and provides models per each one. The implementation viewpoint is focused on the technologies and the system components that are required for implementing the functionalities prescribed by the usage and functional viewpoints. Thus, it provides not only the description of the IIoT system general architecture (*i.e.* its structure and the distribution of components, and the topology by which they are interconnected), but includes a description of interfaces and protocols as well. Roughly speaking, two different kinds of information are transferred in IIoT systems, depending on if the data have to be processed yet (data flow) or they are the results of some elaborations (control flow).

Some architectural patterns are also emerging and providing coherent system implementations and paving the way to innovative business models and services, usually in a multiple-tier arrangement, dictated by the very heterogeneous devices and networks. In the widely accepted three-tier pattern [25], edge, platform, and enterprise tiers are connected by proximity, access, and service networks. The edge defines the domain in which IIoT components interact one with each other. Thus, it consists of sensors, controllers, actuators interconnected by independent local area networks (the proximity networks, usually in the form of fieldbuses) to an edge gateway, which in turn connects to larger networks (access network) of the platform tier, providing global coverage. Finally, the platform tier leverages on the service network to establish links with the enterprise tier that implements domain-specific applications and provides end user interfaces. The Fig. 2) tries to graphically depict the complexity of the IIoT hybrid architecture; in particular, the increased latency and data aggregation of the different tiers is highlighted.

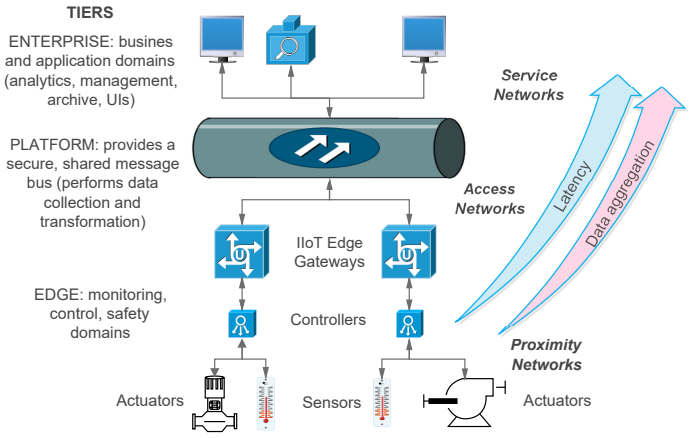

Fig. 2. The three-tier IIoT architecture.

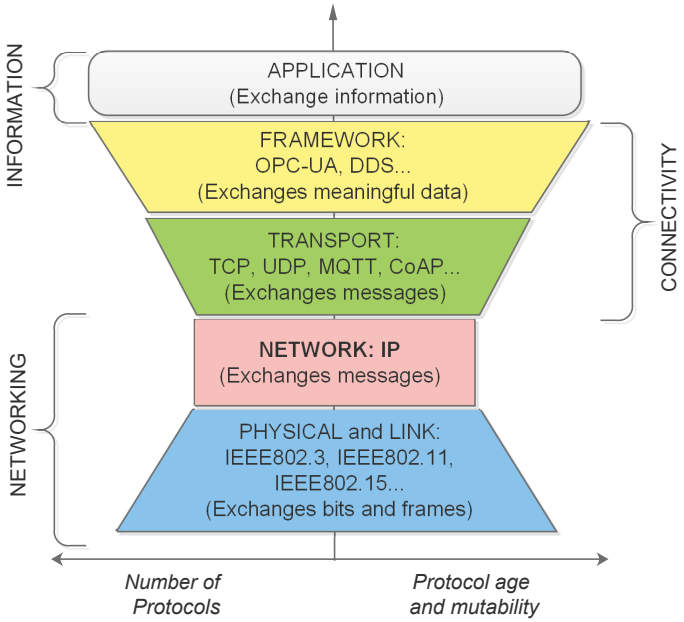

Fig. 3. The hourglass-shaped IIoT protocol stack.

B. The IIoT Connectivity

The connectivity of today's IIoT varies depending on which combination of backbone and edge architecture is useful in a given situation, and a combination of wireless and/or wired technologies is adopted. A key goal is to avoid isolated systems based on proprietary solutions and enable data sharing and interoperability among these closed subsystems (brownfield) and the yet-to-come applications (greenfield), within and across industries. Neither the seven-layer Open Systems Interconnect (OSI) nor the five-layer Internet model is adequate to take into account the distributed nature of sensors, controllers, gateways and other components involved in IIoT and different layering is required. The IIoT initiatives feasibility requires communication protocols able to support efficient, timely and ubiquitous information aggregation and availability. Lower levels of the stack must adequately respond to scalability and flexibility requirements. Upper levels must allow so called "smart devices" (i.e. offering both computation and communication capabilities) to transport "smart data", not limited to the information of interest but also providing awareness of the users they are intended to and all the semantic rules to be correctly understood at destinations as well. Three macro layers can be identified, i.e. networking (dealing with frames and packets), connectivity (dealing with messages) and information (dealing with end-user data structures). The protocol heterogeneity of the IIoT is mirrored in a hourglass-shaped stack (see Fig. 3). The neck is represented by the network layer, *i.e.* the Internet (and its different flavors, as IPv4, IPv6, 6LowPAN, RPL, *etc.*), but above and below sublayers are not yet clearly defined, despite they are of critical importance for ensuring interoperability at different levels.

Additionally, it is worth mentioning that most of current industrial applications exploit fieldbuses, each having its own ecosystem, thus providing poor interoperability. Fieldbuses are vertical solutions covering most of the functionalities of the communication stack. Fortunately, latest technologies (e.g. the many different flavors of the real-time Ethernet solutions) natively adopt Ethernet and IP protocols, thus making it easier to provide technical interoperability, *i.e.* the ability to share packets in a common format [26]. Due to its full IP compatibility and incorporation of the Common Industrial Protocol (CIP), and reliance on standard Internet and Ethernet technology (IEEE 802.3 combined with the TCP/IP Suite), EtherNet/IP makes itself a particularly suitable for IIoT. As an example, myriads of motion applications in industries feature a bevy of connected components – from I/O blocks and vision sensors to servo and variable frequency drives. EtherNet/IP can unite all of these moving parts via CIP communications running on Ethernet [27]. Since it is built on the IP suite, EtherNet/IP is gaining momentum from the development and refinement of associated protocols. In addition to TCP/UDP at the transport layer, it can access higher-level functionality through HTTP. Connectivity between industrial equipment, Ethernet networks and the Internet can enable time-sensitive communications to streamline plant operations, thereby enabling real-time manufacturing for enterprises with global supply chains.

1) Stack Lower Layers: In IIoT stack, the lowest layer is the physical one, which refers to the exchange of physical signals on media linking the participants. Above it lies the link layer, which connects adjacent participants allowing to exchange frames by means of signaling protocols. It has to be noticed that the already available solutions explicitly designed for the industrial market have some limits. Well-accepted standards defined in the IEC62591 and IEC62743 (commercially known as WirelessHART and ISA100.11a) are based on IEEE802.15.4 compliant radio and are not designed to connect a large number of devices, as in typical IIoT applications. Consequently, several independent networks must be deployed, each one with its own IIoT gateway. On the contrary, Low-Power Wide-Area Network (LPWAN) solutions are gaining momentum in recent years for occupying the lower two levels of the protocol stack, with multiple competing technologies being offered or under development [28].

LPWANs allow to communicate over long distances (several kilometers) at very low transmission power. SigFox [29] and

LoRaWAN [30] are two of the most interesting proposals [31]–[33]. However, SigFox, based on ultra narrowband technology (i.e. communication channels with a bandwidth on the order of 100Hz), is mainly intended for smart city applications, *e.g.* smart metering, since a device can send at most 140 messages per day, each one typically having 3s air time. Thus it is not suitable for many industrial applications that require real-time performance or frequent sampling. LoRaWAN (maintained by the LoRa alliance) leverages on proprietary LoRa radios and offers 125kHz or 250kHz-wide channels and low data rate (from about 10kbps down to less than 400bps). It has been demonstrated that by mimicking the time-slotted channel hopping of typical wireless industrial communications, thousand of communication opportunities per second are affordable [34]. As a final remark, it has to be highlighted that LPWANs generally operate in the sub-GHz region, that ensures good coverage but is often limited by duty cycled transmission of 1% or 0.1% or "Listen Before Talk" (LBT) medium access strategy. Also, both SigFox and LoRaWAN are primarily uplink-only. LoRaWAN can enable bidirectional communication, but it has to rely on time synchronized beacons and schedules, which is an overhead. The recently developed SNOW [35]–[38] is an LPWAN that enables concurrent bidirectional communications, thus making it suitable for control applications. However, SNOW operates over the TV white spaces and thus its performance depends on the availability of white spaces.

The use of unlicensed spectrum has raised certain reliability issues, since there is no guarantee of service availability, in addition to the aforementioned duty-cycle and LBT regulations. For this reason, fifth generation cellular access (5G) is often envisioned as a viable IIoT solution, in addition to regular telecommunication applications using the cellular infrastructure. Currently there is no finalized standard for 5G (which actually is an umbrella for many specifications). However, the cost of technical solutions to be applied at the physical layer to satisfy industrial needs can be an important issue. Only a sound business model and a strong argument for using licensed frequency bands (both missing today) could bring market acceptance within industrial automation for 5G [4]. Narrowband LPWAN technology standard to operate on cellular infrastructure and bands as NB-IoT received attention recently, but despite its potential, there are some issues regarding scalability, and network resource slicing between IoT applications and other broadband services that need further studies [39]. In licensed cellular spectrum, EC-GSM-IoT [40] and LTE Cat M1 (LTE-Advanced Pro) [41] are also under development. A key requirement of all these technological solutions is that they need cellular infrastructure.

Bluetooth low energy (BLE) [42] is another interesting alternative for IIoT since it offers ultra-low power consumption but the initial doubts for BLE was due to its range limitations since it only supports star network and limited number of devices [43]. To overcome those limitations, BLE mesh networking standard was recently released and initially considered for home automation. The main challenge with BLE mesh networking targeting real-time communication is that the connection establishment procedure introduces a long delay (e.g., several hundred ms). To overcome this problem, many upper layer protocols such as mesh and beacon try to leverage on the connection-less scheme since there is no need to establish connections before sending data. However, this does not ensure reliable communication due to lack of a good medium access control. Besides, the throughput is much lower than 1 Mbps since there is a limitation of sending packet in this bearer, i.e., at least 20 ms interval is required in order to reduce intra-interference and avoid collisions. Recently there has been some interesting work about using BLE mesh networking for real-time communication targeting low latency applications in industrial automation. In [44], the authors presented a real-time protocol aimed to overcome the problem with range limitations of mesh technology and support bounded real-time traffic. Their protocol exploits time division multiple access (TDMA) with an optimized transmission allocation to provide data packets with real-time support. It works on standard BLE devices. In [45], the authors presented a bandwidth reservation mechanism for partitioning the radio transceiver between two protocols, namely the BLE and a real-time custom protocol.

2) Stack Upper Layers: The aim of upper layers of the IIoT stack is to facilitate/ensure so called syntactic interoperability, *i.e.* the capability to use a common data structure and set of rules for information exchanges [46], [47]. It is the actual application that finally provides the semantic interoperability, *i.e.* the capability to interpret exchanged data unambiguously [26]. In light of this requirement, the Industrial Internet Consortium proposed to separate upper layer protocols into just two levels; the lower is occupied by the transport layer, that is in charge of exchanging variable length messages among the involved applications; the upper constitutes the framework layer, which manages the transfer of structured data having higher abstraction (*e.g.* state, events, streams, etc.). According to this classification, the transport layer is loosely related to the transport layer of OSI (and Internet) model; indeed UDP and TCP are foundations for other transport protocols. However, some functionalities of the session, presentation and application layers are included as well.

A well-accepted and widely used solution for implementing horizontal integration relies on messaging protocols (often implemented by message oriented middleware). These protocols support the publisher/subscriber paradigm, where both sides of the actual data exchange are in general not directly connected. The application that wants to publish a message connects to a so-called message queue broker for placing it in a queue; subsequently, subscribers automatically receive the message as a push notification. The delivering modality is said to be persistent if it survives a broker failure. Messaging solutions ensure scalability since the applications do not have to know each other. Today, a prevailing messaging protocol is MQTT (Message Queue Telemetry Transport), standardized by the OASIS alliance. A different approach relies on request/response data delivery, and synchronous or asynchronous data exchanges are permitted. In the synchronous data exchanges, the requestor waits for replies before issuing the next request. In an asynchronous case, the reply is returned at some unknown later time to the requestor. A well-known example of request/response protocol is CoAP (Constrained

Application Protocol) defined by the the IETF Constrained RESTful Environments (CORE) working group [47].

The framework layer provides services to the above application and manages the lifecycle of any piece of data from the creation to the deletion. Protocols at this level offer the ability to discover and identify data objects and can understand the transported data meaning (*i.e.* are not opaque). This awareness is exploited for optimally delivering the information at the destination. The open platform communications - unified architecture (OPC-UA, a multi-part document set managed by the OPC foundation, formally known as the IEC62541) is an example of such a framework. It describes a Service Oriented Architecture (SOA) based on client/server architecture in which the server models data, information, processes and systems as objects that are presented to clients together with services that the client can use.

C. The Standardization of IIoT

Standardization is an important step for a technology to be widely supported and well-accepted. Interesting to note, most of the past standardization activities focused on very specific domains, thus resulting in disjoint and somewhat redundant development. The standardization process has to face several challenges; currently there is a plethora of competing standardization bodies and consortia initiatives at every layer of the IIoT stack referring to a variety of fragmented, often inconsistent and opponent requirements. Obviously, such an approach is detrimental to IIoT, whose fundamental aim is to bring together and share information coming from very heterogeneous things. The actual fragmentation is effectively highlighted by the ETSI technical report ETSI TR 103375, whose aim is to provide the roadmaps of the IoT standards. Generally speaking, the ongoing standardization activities include horizontal standards, aiming at ensuring interoperability; vertical standards, aiming at identifying requirements of individual applications and use cases; and promotional activities, supported by industrial consortia and government groups.

Focusing on industrial applications, the most significant and important efforts are those carried out by the IEC (International Electrotechnical Commission), which created many different Study Groups and Technical Committees on the subject and published a couple of white papers about IIoT and the smart factory with the aim of assessing potential global needs, benefits, concepts and pre-conditions for the factory of the future. It is worth noting that, regarding the connectivity issues, the aforementioned IEC62541 is the only standard originated in the industrial vertical context.

Standardization activities for 5G targeting IIoT and critical communication is ongoing in 3GPP and falls under the umbrella of *Ultra reliable Low Latency Communications* (URLLC) with the aim of providing 1 ms latency. One way to reduce the latency in URLLC is to provide a reliable transmission time interval (TTI) operation.

Considering that a relevant part of IIoT communications will probably be implemented as wireless links, coexistence issues arise as well. The IEC62657 provides a sort of glossary of industrial automation requirements for harmonizing concepts and terms of the telecommunication world and defines coexistence parameters (in the form of templates) and guidelines for ensuring wireless coexistence within industrial automation applications along the whole lifecycle of the plant.

IV. Opportunities and Challenges

A key reason for adopting IIoT by manufacturers, utility companies, agriculture producers and healthcare providers is to increase productivity and efficiency through smart and remote management. As an example, Thames Water [48], the largest provider of drinking and waste-water services in the UK, is using sensors, and real-time data acquisition and analytics to anticipate equipment failures and provide fast response to critical situations, such as leaks or adverse weather events. The utility firm has already installed more than 100,000 smart meters in London, and it aims to cover all customers with smart meters by 2030. With more than 4,200 leaks detected on customer pipes so far, this program has already saved an estimated 930,000 liters of water per day across London. As another example, the deployment of 800 HART devices for real-time process management at Mitsubishi chemical plant in Kashima, Japan has been increasing the production performance by saving US$20-30,000 per day that also averted a $3million shutdown [49].

Precision agriculture powered by IIoT can help farmers better measure agricultural variables such as soil nutrients, fertilizer used, seeds planted, soil water, and temperature of stored produce, allowing to monitor down to the square foot through a dense sensor deployment, thereby almost doubling the productivity [50]–[52]. Companies like Microsoft (FarmBeats project [53], [54]), Climate Corp [55], AT&T [56], and Monsanto [57] are promoting agricultural IoT. IIoT can also significantly impact the healthcare field. In hospitals, human or technological errors caused by false alarms, slow response, and inaccurate information are still a major reason of preventable death and patient suffering. By connecting distributed medical devices using IIoT technologies, hospitals can significantly overcome such limitations, thereby improving patient safety and experiences, and more efficiently using the resources.

IIoT also provides opportunities to enhance efficiency, safety, and working conditions for workers. For example, using unmanned aerial vehicles (UAVs) allows inspecting oil pipelines, monitoring food safety using sensors, and minimizing workers' exposure to noise, and hazardous gases or chemicals in industrial environments. Schlumberger, for example, is now monitoring subsea conditions using unmanned marine vehicles, which can travel across oceans collecting data for up to a year without fuel or crew, moving under power generated from wave energy [58]. Through remote monitoring and sensing powered by IIoT, mining industries can dramatically decrease safety-related incidents, while making mining in harsh locations more economical and productive. For example, Rio Tinto, a leading mining company, intends its automated operations in Australia to preview a more efficient future for all of its mines to reduce the need for human miners [59].

Despite the great promise, there are many challenges in realizing the opportunities offered by IIoT, which should be

addressed in the future research. The key challenges stem from the requirements in energy-efficient operation, real-time performance in dynamic environments, the need for coexistence and interoperability, and maintaining the security of the applications and users' privacy as described below.

A. Energy Efficiency

Many IIoT applications need to run for years on batteries. This calls for the design of low-power sensors which do not need battery replacement over their lifetimes. This creates a demand for energy-efficient designs. To complement such designs, upper-layer approaches can play important roles through energy-efficient operation. Many energy efficient schemes for wireless sensor network (WSN) have been proposed in recent years [60], but those approaches are not immediately applicable to IIoT. IIoT applications typically need a dense deployment of numerous devices. Sensed data can be sent in queried form or in a continuous form which in a dense deployment can consume a significant amount of energy. Green networking is thus crucial in IIoT to reduce power consumption and operational costs. It will lessen pollution and emissions and make the most of surveillance and environmental conservation. LPWAN IoT technologies achieve low-power operation using several energy-efficient design approaches. *First*, they usually form a star topology, which eliminates the energy consumed through packet routing in multi-hop networks. *Second*, they keep the node design simple by offloading the complexities to the gateway. *Third*, they use narrowband channels, thereby decreasing the noise level and extending the transmission range [35], [61].

Although there are numerous methods to achieve energy efficiency, such as using lightweight communication protocols or adopting low-power radio transceivers as described above, the recent technology trend in energy harvesting provides another fundamental method to prolong battery-life. Thus, energy harvesting is a promising approach for the emerging IIoT. Practically, energy can be harvested from environmental sources, namely, thermal, solar, vibration, and wireless radio-frequency (RF) energy sources. Harvesting from such environmental sources is dependent on the presence of the corresponding energy source. However, RF energy harvesting may provide benefits in terms of being wireless, readily available in the form of transmitted energy (TV/radio broadcasters, mobile base stations and hand-held radios), low cost, and in terms of small form factor of devices.

B. Real-Time Performance

IIoT devices are typically deployed in noisy environments for supporting mission- and safety-critical applications, and have stringent timing and reliability requirements on timely collection of environmental data and proper delivery of control decisions. The QoS offered by IIoT is thus often measured by how well it satisfies the end-to-end (e2e) deadlines of the real-time sensing and control tasks executed in the system [62], [63].

Time-slotted packet scheduling in IIoT plays a critical role in achieving the desired QoS. For example, many industrial wireless networks perform network resource management via static data link layer scheduling [64]–[71] to achieve deterministic e2e real-time communication. Such approaches typically take a periodic approach to gathering the network health status, and then recompute and distribute the updated network schedule information. This process however is slow, not scalable and incurs considerable network overhead. The explosive growth of IIoT applications especially in terms of their scale and complexity has dramatically increased the level of difficulty in ensuring the desired real-time performance. The fact that most IIoT must deal with unexpected disturbances further aggravate the problem.

Unexpected disturbances can be classified into *external* disturbances from the environment being monitored and controlled (*e.g.*, detection of an emergency, sudden pressure or temperature changes) and *internal* disturbances within the network infrastructure (*e.g.*, link failure due to multi-user interference or weather related changes in channel SNR). In response to various internal disturbances, many centralized scheduling approaches [72]–[77] have been proposed. There are also a few works on adapting to external disturbances in critical control systems. For example, rate-adaptive and rhythmic task models are introduced in [78] and [79], respectively, which allow tasks to change periods and relative deadlines in some control systems such as automotive systems.

Given the requirement of meeting e2e deadlines, the aforementioned approaches for handling unexpected disturbances are almost all built on a centralized architecture. Hence, most of them have limited scalability [80]. The concept of distributed resource management is not new. In fact, distributed approaches have been investigated fairly well in the wireless network community (e.g., [81]–[85]). However, these studies typically are not concerned with real-time e2e constraints. A few which consider real-time constraints mainly focus on soft real-time requirements and do not consider external disturbances that IIoT must have to deal with. Only recently, we have started to see some hybrid and fully distributed resource management approaches for IIoT [86], [87]. However how to ensure bounded response time to handle concurrent disturbances is still an open problem.

C. Coexistence and Interoperability

With the rapid growth of IIoT connectivity, there will be many coexisting devices deployed in close proximity in the limited spectrum. This brings forth the imminent challenge of coexistence in the crowded ISM bands. Thus, interference between devices must be handled to keep them operational. Existing and near future IIoT devices will most likely have limited memory and intelligence to combat interference or keep it to a minimum. While there exists much work on wireless coexistence considering WiFi, IEEE 802.15.4 networks, and Bluetooth (see surveys [88]–[91]), they will not work well for IIoT. Due to their dense and large-scale deployments, these devices can be subject to an unprecedented number of interferers. Technology-specific features of each IIoT technology may introduce additional challenges.

To ensure good coexistence it will become important that future IIoT devices can detect, classify and mitigate exter-

nal interference. Recently, some work regarding classifying interference via spectrum sensing [92] on IIoT devices has been presented but most of the existing work fails since a very long sampling window is needed and the proposed spectrum sensing methods need much more memory than what is available in existing commercial IIoT devices. Hence, in [93] a promising method was presented and implemented in Crossbow's TelosB mote CA2400 which is equipped with Texas Instrument CC2420 transceiver. That method manages to classify external interference by using support vector machines with a sensing duration below 300 ms. Moreover, existing devices based on IEEE 802.15.4 standards do not have any forward error correcting (FEC) capabilities to improve the reliability of the data packet. There exists some work that investigated error control codes for industrial WSNs and the results clearly show that FEC will improve reliability and the coexistence [94]–[96]. However, most of the available FEC methods are optimized for long packets. Given that IIoT communication will mainly consist of short packets (50-70 bytes) and many applications are time-critical, more research is needed to find good error correcting codes for IIoT communication [97]. If the research of error correcting codes for IIoT devices should be successful, it is also important that more emphasis be given on investigating and understanding the complex radio environment where many of these IIoT devices will be deployed [98], [99].

The rapid growth of IIoT technologies also brings forth the requirements of interoperability. Namely, in the future, a fully functional digital ecosystem will require seamless data sharing between machines and other physical systems from different manufacturers. The lack of interoperability among IIoT devices will significantly increase the complexity and cost of IIoT deployment and integration. The drive towards seamless interoperability will be further complicated by the long life span of typical industrial equipment, which would require costly retrofitting or replacement to work with the latest technologies.

The challenges of device diversity in IIoT can be addressed along three dimensions: multimode radios, software flexibility, cross-technology-communication [100]. Multimode radios allow diverse IIoT devices to talk to each other. Software flexibility enables support for multiple protocols, connectivity frameworks and cloud services. Recently, cross-technology-communication [101] without the assistance of additional hardware has been studied for communication across WiFi, ZigBee, and Bluetooth devices. Such approaches are specific to technologies, and thus future research is needed to enable cross-technology-communication in IIoT devices.

D. Security and Privacy

Besides the requirements of energy-efficiency and real-time performance, security is another critical concern in IIoT. In general, IIoT is a resource-constrained communication network which largely relies on low-bandwidth channels for communication among lightweight devices regarding CPU, memory and energy consumption [102]. For this reason, traditional protection mechanisms are not sufficient to secure the complex IIoT systems, such as secure protocols [103], lightweight cryptography [104] and privacy assurance [105]. To secure the IIoT infrastructure, existing encryption techniques from industrial WSNs may be reviewed before applied to build IIoT secure protocols. For instance, scarce computing and memory resources prevent the use of resource-demanding crypto-primitives, *e.g.* Public-Key Cryptography (PKC). This challenge is more critical in the applications of massive data exchanged with real-time requirements. To address privacy and security threats in IIoT, one can argue for a holistic approach as pointed out in [106]. This means that aspects such as platform security, secure engineering, security management, identity management and industrial rights management must be taken into account, throughout the whole life cycle of the systems and products.

There exist several security properties to consider when designing secure IIoT infrastructure [107]:

1) IIoT devices need to be tamper resistant against potential physical attacks, such as unauthorized re-programming and passive secret stealing while allowing the authorized users to update the security firmware on the device.
2) The storage of IIoT device should be protected against adversary by keeping the data encrypted to keep the confidentiality.
3) The communication network among the IIoT devices should be secured to keep confidentiality and integrity.
4) The IIoT infrastructure needs efficient identification and authorization mechanisms, so that only authorized entities can access the IIoT resource.
5) The system should be available within normal operation, even with the physical damage to the devices by malicious users. This guarantees the robustness of IIoT.

Typically, symmetric-key cryptography can provide a lightweight solution for IIoT devices. However, both the key storage and the key management are big issues if using symmetric-key encryption, especially when considering low-capacity devices.

Additionally, if one device in IIoT is compromised, it may leak all other keys. Public-key cryptography generally provides more secure features, and low storage requirements, but suffers from high computational overhead due to complex encryption. Thus, reducing the overhead of complex security protocols for public-key cryptosystems remains a major challenge for IIoT security. In PKC, Elliptic-Curve Cryptography (ECC) provides a lightweight solution regarding computational resources. It provides a smaller key size, reducing storage and transmission requirements.

In IIoT systems, it is important to provide the identification to get the legal access. The secure IIoT infrastructure must ensure the object identification regarding the integrity of records used in the naming systems, such as Domain Name System (DNS). The DNS system can provide name translation services to the Internet user, however, it is in an insecure way which remains vulnerable to various attacks by deliberated adversary [108]. This challenge stays valid even for a bounded and closed environment. Thus, without the integrity protection of the identification, the whole naming system is still insecure. Security extensions to DNS, like, Domain Name Service

Security Extension (DNSSEC) increases security and is documented in IETF RFC4033 [109]. However, due to its high computation and communication overhead, it is challenging to directly apply DNSSEC to the IIoT infrastructure.

IIoT devices should follow specific schemes and rules for authentication to exchange/publish their data. Due to the resource constraints of the IIoT devices, low-cost authentication schemes have not been provided as much as needed [110]. Although public-key cryptography systems provide the methods for constructing authentication and authorization schemes, it fails to provide a global root certification authority (global root CA), which largely hinders many theoretically feasible schemes from actually being deployed. Without providing the global root CA, it becomes very challenging to design a secure authentication system in IIoT. Thus, currently, if we intend to provide the secure authentication for IIoT devices, we have to use the high-cost solutions which is a conflict with the main goal of the lightweight principle of IIoT [111]. Furthermore, it is a big challenge to issue a certification to each object in IIoT since the total number of objects could be huge.

Privacy is a very broad and diverse concept. Many definitions and perspectives have been provided in the literature. Generally speaking, privacy in IIoT is the threefold guarantee [112] for: 1) awareness of privacy risks imposed by things and services; 2) individual control over the collection and processing of information; 3) awareness and control of subsequent use and dissemination to any outside entity. The major challenges for privacy lie in two aspects: data collection process and data anonymization process. Typically, data collection process deals with the collectible data and the access control to these data during the data collection from smart things; data anonymization is a process to ensure data anonymity through both cryptographic protection and concealment of data relations. Due to the restrictions on the collection and storage of private information, privacy preservation can be ensured during the data collection. However, given the diversity of the things in data anonymization, different cryptographic schemes may be adopted which is a challenge to privacy preserving. Meanwhile, the collected information needs to be shared among the IIoT devices, and the computation on encrypted data is another challenge for data anonymization.

V. Conclusion

This paper presented an overview of the emerging IIoT solutions. What is proposed as a revolution for the consumer market can be another step of the ever evolving industrial communications world. Several technologies are involved and terms as IoT, IIoT and Industry 4.0 are often misused. In this paper, we have provided a systematic overview of IIoT, focusing on the definition of its architecture and describing the protocol ecosystem which is emerging from standardization efforts. We have also discussed the challenges for its realization. Besides the QoS requirements that characterize industrial communications, IIoT suffers from yet to be considered security challenges that stem from the high sensitivity of the managed information. Furthermore, typical IIoT applications have to deal with constrained resources (both power and computing) and must be operative for extended periods of time, ensuring availability and reliability. We have described the state-of-the-art research and standardization efforts and future research directions to address IIoT challenges.

References

[1] Ericsson, "Cellular networks for massive iot," January 2016, https://www.ericsson.com/assets/local/publications/white-papers/wp_iot.pdf.

[2] F. Group, "WirelessHART specification," 2007, http://www.hartcomm2.org.

[3] "ISA100: Wireless systems for automation," http://www.isa.org/MSTemplate.cfm?MicrositeID=1134&CommitteeID=6891.

[4] M. Gidlund, T. Lennvall, and J. Akerberg, "Will 5g become yet another wireless technology for industrial automation?" in *IEEE International Conference on Industrial Technology (ICIT)*, 2017, pp. 1319–1324.

[5] J. Akerberg, M. Gidlund, and M. Bjorkman, "Future research challenges in wireless sensor and actuator networks targeting industrial automation," in *Proceedings of the 9th IEEE International Conference on Industrial Informatics*, 2011, pp. 410–415.

[6] M. R. Palattella, M. Dohler, A. Grieco, G. Rizzo, J. Torsner, T. Engel, and L. Ladid, "Internet of things in the 5G era: Enablers, architecture, and business models," *IEEE Journal on Selected Areas in Communications*, vol. 34, no. 3, pp. 510–527, 2016.

[7] D. Bandyopadhyay and J. Sen, "Internet of things: Applications and challenges in technology and standardization," *Wireless Personal Communications*, vol. 58, no. 1, pp. 49–69, 2011.

[8] M. R. Palattella, P. Thubert, X. Vilajosana, T. Watteyne, Q. Wang, and T. Engel, *Internet of Things. IoT Infrastructures: Second International Summit*, 2016.

[9] L. D. Xu, W. He, and S. Li, "Internet of things in industries: A survey," vol. 10, no. 4, pp. 2233–2243.

[10] M. Wollschlaeger, T. Sauter, and J. Jasperneite, "The future of industrial communication: Automation networks in the era of the internet of things and industry 4.0," *IEEE Industrial Electronics Magazine*, vol. 11, no. 1, pp. 17–27, 2017.

[11] W. He and L. Xu, "A state-of-the-art survey of cloud manufacturing," *International Journal of Computer Integrated Manufacturing*, vol. 28, no. 3, pp. 239–250, 2015. [Online]. Available: https://doi.org/10.1080/0951192X.2013.874595

[12] I. Lee, "An exploratory study of the impact of the internet of things iot on business model innovation: Building smart enterprises at fortune 500 companies," *Int. J. Inf. Syst. Soc. Chang.*, vol. 7, no. 3, pp. 1–15, Jul. 2016. [Online]. Available: http://dx.doi.org/10.4018/IJISSC.2016070101

[13] P. O'Donovan, K. Leahy, K. Bruton, and D. T. J. O'Sullivan, "An industrial big data pipeline for data-driven analytics maintenance applications in large-scale smart manufacturing facilities," *Journal of Big Data*, vol. 2, no. 1, p. 25, Nov 2015. [Online]. Available: https://doi.org/10.1186/s40537-015-0034-z

[14] T. Qu, S. P. Lei, Z. Z. Wang, D. X. Nie, X. Chen, and G. Q. Huang, "Iot-based real-time production logistics synchronization system under smart cloud manufacturing," *The International Journal of Advanced Manufacturing Technology*, vol. 84, no. 1, pp. 147–164, Apr 2016. [Online]. Available: https://doi.org/10.1007/s00170-015-7220-1

[15] S. G. Pease, R. Trueman, C. Davies, J. Grosberg, K. H. Yau, N. Kaur, P. Conway, and A. West, "An intelligent real-time cyber-physical toolset for energy and process prediction and optimisation in the future industrial internet of things," *Future Generation Computer Systems*, vol. 79, pp. 815 – 829, 2018. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167739X1630382X

[16] T. H. Szymanski, "Supporting consumer services in a deterministic industrial internet core network," *IEEE Communications Magazine*, vol. 54, no. 6, pp. 110–117, June 2016.

[17] M. Weyrich and C. Ebert, "Reference architectures for the internet of things," *IEEE Software*, vol. 33, no. 1, pp. 112–116, 2016.

[18] X. Jia, Q. Feng, T. Fan, and Q. Lei, "Rfid technology and its applications in internet of things (iot)," in *Proceedings of the 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet)*, 2012, pp. 1282–1285.

[19] M. C. Domingo, "An overview of the internet of things for people with disabilities," *Journal of Network and Computer Applications*, vol. 35, no. 2, pp. 584–596, 2012.

[20] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," *Computer networks*, vol. 54, no. 15, pp. 2787–2805, 2010.

[21] C. H. Liu, B. Yang, and T. Liu, "Efficient naming, addressing and profile services in internet-of-things sensory environments," *Ad Hoc Networks*, vol. 18, pp. 85–101, 2014.

[22] L. Da Xu, W. He, and S. Li, "Internet of things in industries: A survey," *IEEE Transactions on industrial informatics*, vol. 10, no. 4, pp. 2233–2243, 2014.

[23] H. Flatt, S. Schriegel, J. Jasperneite, H. Trsek, and H. Adamczyk, "Analysis of the cyber-security of industry 4.0 technologies based on rami 4.0 and identification of requirements," in *IEEE 21st Int. Conf. on Emerging Tech. and Factory Automation*, 2016, pp. 1–4.

[24] "Industrial internet reference architecture," http://www.iiconsortium.org/IIRA.htm.

[25] *IoT 2020: Smart and Secure IoT Platform*. International Electrotechnical Commission, 2016.

[26] J. Kiljander, A. Delia, F. Morandi, P. Hyttinen, J. Takalo-Mattila, A. Ylisaukko-Oja, J. P. Soininen, and T. S. Cinotti, "Semantic interoperability architecture for pervasive computing and internet of things," *IEEE Access*, vol. 2, pp. 856–873, 2014.

[27] http://www.industrial-ip.org/en/industrial-ip/ethernet-ip/ethernetip-infographic.

[28] D. Ismail, M. Rahman, and A. Saifullah, "Low-power wide-area networks: Opportunities, challenges, and directions," in *Proceedings of the Workshop Program of the 19th International Conference on Distributed Computing and Networking*, ser. Workshops ICDCN '18, 2018, pp. 8:1–8:6.

[29] Sigfox, "Sigfox - the global communications service provider for the internet of things (iot)," http://sigfox.com.

[30] lora alliance, "LoRaWAN," https://www.lora-alliance.org.

[31] W. Yang, M. Wang, J. Zhang, J. Zou, M. Hua, T. Xia, and X. You, "Narrowband wireless access for low-power massive internet of things: A bandwidth perspective," *IEEE Wireless Communications*, vol. 24, no. 3, pp. 138–145, 2017.

[32] P. Ferrari, A. Flammini, M. Rizzi, E. Sisinni, and M. Gidlund, "On the evaluation of lorawan virtual channels orthogonality for dense distributed systems," in *IEEE International Workshop on Measurement and Networking (M&N)*, 2017, pp. 1–6.

[33] M. Rizzi, P. Ferrari, A. Flammini, and E. Sisinni, "Evaluation of the iot lorawan solution for distributed measurement applications," *IEEE Transactions on Instrumentation and Measurement*, vol. 66, no. 12, pp. 3340–3349, Dec 2017.

[34] M. Rizzi, P. Ferrari, A. Flammini, E. Sisinni, and M. Gidlund, "Using lora for industrial wireless networks," in *IEEE 13th International Workshop on Factory Communication Systems (WFCS)*, 2017, pp. 1–4.

[35] A. Saifullah, M. Rahman, D. Ismail, C. Lu, R. Chandra, and J. Liu, "SNOW: Sensor network over white spaces," in *The 14th ACM Conf. on Embedded Network Sensor Systems (SenSys)*, 2016, pp. 272–285.

[36] A. Saifullah, M. Rahman, D. Ismail, C. Lu, J. Liu, and R. Chandra, "Enabling reliable, asynchronous, and bidirectional communication in sensor networks over white spaces," in *The 15th ACM Conference on Embedded Network Sensor Systems (SenSys)*, 2017, pp. 1–14.

[37] M. Rahman and A. Saifullah, "Integrating low-power wide-area networks in white spaces," in *ACM/IEEE Conference on Internet-of-Things Design and Implementation (IoTDI)*, 2018.

[38] A. Saifullah, M. Rahman, D. Ismail, C. Lu, J. Liu, and R. Chandra, "Low-power wide-area networks over white spaces," *ACM/IEEE Transactions on Networking*, 2018.

[39] Y. D. Beyene, R. Jantti, O. Tirkkonen, K. Ruttik, S. Iraji, A. Larmo, T. Tirronen, and a. J. Torsner, "Nb-iot technology overview and experience from cloud-ran implementation," *IEEE Wireless Communications*, vol. 24, no. 3, pp. 26–32, 2017.

[40] GSMA, "3gpp low power wide area technologies," October 2016, https://www.gsma.com/iot/wp-content/uploads/2016/10/3GPP-Low-Power-Wide-Area-Technologies-GSMA-White-Paper.pdf.

[41] u blox, "Lte cat m1," https://www.u-blox.com/en/lte-cat-m1.

[42] Bluetooth-SIG, "Bluetooth core specification version 5.0," 2016.

[43] R. Rondón, M. Gidlund, and K. Landernäs, "Evaluating bluetooth low energy suitability for time-critical industrial iot applications," *International Journal of Wireless Information Networks*, vol. 24, no. 3, pp. 278–290, Sep 2017.

[44] G. Patti, L. Leonardi, and L. L. Bello, "A bluetooth low energy real-time protocol for industrial wireless mesh networks," in *IECON 2016 - 42nd Annual Conference of the IEEE Industrial Electronics Society*, Oct 2016, pp. 4627–4632.

[45] M. Marinoni, A. Biondi, P. Buonocunto, G. Franchino, D. Cesarini, and G. Buttazzo, "Real-time analysis and design of a dual protocol support for bluetooth le devices," *IEEE Transactions on Industrial Informatics*, vol. 13, no. 1, pp. 80–91, Feb 2017.

[46] A. Al-Fuqaha, A. Khreishah, M. Guizani, A. Rayes, and M. Mohammadi, "Toward better horizontal integration among iot services," *IEEE Communications Magazine*, vol. 53, no. 9, pp. 72–79, 2015.

[47] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of things: A survey on enabling technologies, protocols, and applications," *IEEE Communications Surveys Tutorials*, vol. 17, no. 4, pp. 2347–2376, 2015.

[48] J. P. Tomas, "Thames water rolls out smart meter project in london," 2017, https://wiprodigital.com/cases/progressive-metering-a-utilitys-strategic-move-into-predictive-planning/.

[49] http://en.hartcomm.org/hcp/tech/applications/applications_success_mitsubishi_chemical.html.

[50] M. H. Almarshadi and S. M. Ismail, "Effects of precision irrigation on productivity and water use efficiency of alfalfa under different irrigation methods in arid climates," *Journal of Applied Sciences Research*, vol. 7, no. 3, pp. 299–308, 2011.

[51] H.-J. Kim, K. A. Sudduth, and J. W. Hummel, "Soil macronutrient sensing for precision agriculture," *Journal of Environmental Monitoring*, vol. 11, no. 10, pp. 1810–1824, 2009.

[52] N. D. Mueller, J. S. Gerber, M. Johnston, D. K. Ray, N. Ramankutty, and J. A. Foley, "Closing yield gaps through nutrient and water management," *Nature*, vol. 490, no. 7419, pp. 254–257, 2012.

[53] D. Vasisht, Z. Kapetanovic, J. Won, X. Jin, R. Chandra, S. Sinha, A. Kapoor, M. Sudarshan, and S. Stratman, "Farmbeats: An iot platform for data-driven agriculture," in *14th USENIX Symp. on Net. Syst. Design and Implementation (NSDI)*, 2017, pp. 515–529.

[54] Microsoft, "FarmBeats: IoT for agriculture," https://www.microsoft.com/en-us/research/project/farmbeats-iot-agriculture/.

[55] C. Corporation, "Data-driven agricultural decisions and insights to maximize every acre," https://www.climate.com.

[56] AT&T M2X, "Agriculture iot software as a service (saas)," https://m2x.att.com/iot/industry-solutions/iot-data/agriculture/.

[57] J. Hawn, "Agricultural iot promises to reshape farming," RCR Wireless News, November 2015, https://www.rcrwireless.com/20151111/internet-of-things/agricultural-internet-of-things-promises-to-reshape-farming-tag15.

[58] Schlumberger, "Schlumberger robotics services," http://www.slb.com/services/additional/robotics-services.aspx.

[59] T. Simonite, "Mining 24 hours a day with robots," MIT Technology Review, December 2016, https://www.technologyreview.com/s/603170/mining-24-hours-a-day-with-robots/.

[60] T. Rault, A. Bouabdallah, and Y. Challal, "Energy efficiency in wireless sensor networks: a top-down survey," vol. 67, pp. 104–122, 07 2014.

[61] 3GPP, "Standardization of NB-IOT completed," June 2016, http://www.3gpp.org/news-events/3gpp-news/1785-nb_iot_complete.

[62] P. Ferrari, A. Flammini, E. Sisinni, D. Brando, and M. Rocha, "Delay estimation of industrial iot applications based on messaging protocols," *IEEE Transactions on Instrumentation and Measurement*, pp. 1–12, 2018.

[63] T. Zheng, M. Gidlund, and J. Akerberg, "Wirarb: A new mac protocol for time critical industrial wireless sensor network applications," *IEEE Sensors Journal*, vol. 16, no. 7, pp. 2127–2139, April 2016.

[64] S. Han, X. Zhu, D. Chen, A. K. Mok, and M. Nixon, "Reliable and real-time communication in industrial wireless mesh networks," in *Proceedings of IEEE Real-Time and Embedded Technology and Applications Symposium (RTAS)*, 2011, pp. 3–12.

[65] Q. Leng, Y.-H. Wei, S. Han, A. Mok, W. Zhang, and M. Tomizuka, "Improving control performance by minimizing jitter in rt-wifi networks," in *IEEE Real-Time Sys. Symp. (RTSS)*, 2014, pp. 63–73.

[66] A. Saifullah, C. Lu, Y. Xu, and Y. Chen, "Real-time scheduling for WirelessHART networks," in *Proceedings of IEEE Real-Time Systems Symposium (RTSS)*, 2010, pp. 150–159.

[67] J. Song, S. Han, A. Mok, D. Chen, M. Lucas, M. Nixon, and W. Pratt, "Wirelesshart: Applying wireless technology in real-time industrial process control," in *Proceedings of IEEE Real-Time and Embedded Technology and Applications Symposium (RTAS)*, 2008, pp. 377–386.

[68] Y.-H. Wei, Q. Leng, S. Han, A. K. Mok, W. Zhang, and M. Tomizuka, "RT-WiFi: Real-time high-speed communication protocol for wireless cyber-physical control applications," in *Proceedings of IEEE Real-Time Systems Symposium (RTSS)*, 2013, pp. 140–149.

[69] A. Saifullah, Y. Xu, C. Lu, and Y. Chen, "End-to-end communication delay analysis in industrial wireless networks," *IEEE Transactions on Computers*, vol. 64, no. 5, pp. 1361–1374, 2014.

[70] A. Saifullah, D. Gunatilaka, P. Tiwari, M. Sha, C. Lu, B. Li, C. Wu, and Y. Chen, "Schedulability analysis under graph routing in WirelessHART networks," in *Proceedings of the IEEE Real-Time Systems Symposium (RTSS)*, 2015, pp. 165–174.

[71] A. Saifullah, S. Sankar, J. Liu, C. Lu, B. Priyantha, and R. Chandra, "CapNet: A real-time wireless management network for data center power capping," in *Proceedings of the IEEE Real-Time Systems Symposium (RTSS)*, 2014, pp. 334–345.

[72] O. Chipara, C. Lu, and G.-C. Roman, "Real-time query scheduling for wireless sensor networks," *IEEE transactions on computers*, vol. 62, no. 9, pp. 1850–1865, 2013.

[73] O. Chipara, C. Wu, C. Lu, and W. Griswold, "Interference-aware real-time flow scheduling for wireless sensor networks," in *the 23rd Euromicro Conf. on Real-Time Sys. (ECRTS)*, 2011, pp. 67–77.

[74] T. L. Crenshaw, S. Hoke, A. Tirumala, and M. Caccamo, "Robust implicit edf: A wireless mac protocol for collaborative real-time systems," *ACM Trans. on Embed. Comp. Sys. (TECS)*, vol. 6, no. 4, p. 28, 2007.

[75] A. Saifullah, C. Wu, P. Tiwari, Y. Xu, Y. Fu, C. Lu, and Y. Chen, "Near optimal rate selection for wireless control systems," *ACM Transactions on Embedded Computing Systems*, vol. 13, no. 4s, pp. 1–25, 2013.

[76] W. Shen, T. Zhang, M. Gidlund, and F. Dobslaw, "Sas-tdma: a source aware scheduling algorithm for real-time communication in industrial wireless sensor networks," *Wireless networks*, vol. 19, no. 6, pp. 1155–1170, 2013.

[77] F. Dobslaw, T. Zhang, and M. Gidlund, "End-to-end reliability-aware scheduling for wireless sensor networks," *IEEE Transactions on Industrial Informatics*, vol. 12, no. 2, pp. 758–767, 2016.

[78] G. C. Buttazzo, E. Bini, and D. Buttle, "Rate-adaptive tasks: Model, analysis, and design issues," in *Design, Automation & Test in Europe Conference & Exhibition (DATE)*. IEEE, 2014, pp. 1–6.

[79] J. Kim, K. Lakshmanan, and R. Rajkumar, "Rhythmic tasks: A new task model with continually varying periods for cyber-physical systems," in *IEEE/ACM Third International Conference on Cyber-Physical Systems (ICCPS)*, 2012, pp. 55–64.

[80] 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," *Proceedings of the IEEE*, vol. 104, no. 5, pp. 1013–1024, 2016.

[81] A. Gupta, X. Lin, and R. Srikant, "Low-complexity distributed scheduling algorithms for wireless networks," *IEEE/ACM Transactions on Networking (TON)*, vol. 17, no. 6, pp. 1846–1859, 2009.

[82] X. Lin and S. B. Rasool, "Constant-time distributed scheduling policies for ad hoc wireless networks," *IEEE Transactions on Automatic Control*, vol. 54, no. 2, pp. 231–242, 2009.

[83] N. Vaidya, A. Dugar, S. Gupta, and P. Bahl, "Distributed fair scheduling in a wireless lan," *IEEE Transactions on Mobile Computing*, vol. 4, no. 6, pp. 616–629, 2005.

[84] K. S. Vijayalayan, A. Harwood, and S. Karunasekera, "Distributed scheduling schemes for wireless mesh networks: A survey," *ACM Computing Surveys (CSUR)*, vol. 46, no. 1, p. 14, 2013.

[85] X. Wu, R. Srikant, and J. R. Perkins, "Scheduling efficiency of distributed greedy scheduling algorithms in wireless networks," *IEEE Transactions on Mobile Computing*, vol. 6, no. 6, pp. 595–605, 2007.

[86] T. Zhang, T. Gong, C. Gu, H. Ji, S. Han, Q. Deng, and X. S. Hu, "Distributed dynamic packet scheduling for handling disturbances in real-time wireless networks," in *IEEE Real-Time and Embed. Tech. and App. Symp. (RTAS)*, 2017, pp. 261–272.

[87] T. Zhang, T. Gong, Z. Yun, S. Han, Q. Deng, and X. S. Hu, "Fd-pas: A fully distributed packet scheduling framework for handling disturbances in real-time wireless networks," in *IEEE Real-Time and Embed. Tech. and App. Symp. (RTAS)*, 2018, pp. 1–12.

[88] D. Yang, Y. Xu, and M. Gidlund, "Coexistence of ieee802.15.4 based networks: A survey," in *Proceedings of the 36th Annual Conference on IEEE Industrial Electronics Society (IECON)*, 2010, pp. 2107–2113.

[89] ——, "Wireless coexistence between ieee 802.11- and ieee 802.15.4-based networks: A survey," *International Journal of Distributed Sensor Networks*, vol. 7, no. 1, p. 912152, 2011.

[90] A. Sikora and V. F. Groza, "Coexistence of ieee802.15.4 with other systems in the 2.4 ghz-ism-band," in *Proceedings of IEEE Instrumentation and Measurement Technology Conference*, vol. 3, 2005, pp. 1786–1791.

[91] L. L. Bello and E. Toscano, "Coexistence issues of multiple co-located ieee 802.15.4/zigbee networks running on adjacent radio channels in industrial environments," *IEEE Transactions on Industrial Informatics*, vol. 5, no. 2, pp. 157–167, 2009.

[92] T. M. Chiwewe, C. F. Mbuya, and G. P. Hancke, "Using cognitive radio for interference-resistant industrial wireless sensor networks: An overview," *IEEE Transactions on Industrial Informatics*, vol. 11, no. 6, pp. 1466–1481, 2015.

[93] S. Grimaldi, A. Mahmood, and M. Gidlund, "An svm-based method for classification of external interference in industrial wireless sensor and actuator networks," *Journal of Sensor and Actuator Networks*, vol. 6, no. 2, p. 9, 2017.

[94] F. Barac, M. Gidlund, and T. Zhang, "Scrutinizing bit- and symbol-errors of ieee 802.15.4 communication in industrial environments," *IEEE Transactions on Instrumentation and Measurement*, vol. 63, no. 7, pp. 1783–1794, 2014.

[95] Y. H. Yitbarek, K. Yu, J. Akerberg, M. Gidlund, and M. Bjorkman, "Implementation and evaluation of error control schemes in industrial wireless sensor networks," in *2014 IEEE International Conference on Industrial Technology (ICIT)*, 2014, pp. 730–735.

[96] F. Barac, M. Gidlund, and T. Zhang, "Ubiquitous, yet deceptive: Hardware-based channel metrics on interfered wsn links," *IEEE Transactions on Vehicular Technology*, vol. 64, no. 5, pp. 1766–1778, 2015.

[97] F. Barac, S. Caiola, M. Gidlund, E. Sisinni, and T. Zhang, "Channel diagnostics for wireless sensor networks in harsh industrial environments," *IEEE Sensors Journal*, vol. 14, no. 11, pp. 3983–3995, 2014.

[98] P. Agrawal, A. Ahlen, T. Olofsson, and M. Gidlund, "Long term channel characterization for energy efficient transmission in industrial environments," *IEEE Transactions on Communications*, vol. 62, no. 8, pp. 3004–3014, 2014.

[99] T. Olofsson, A. Ahlen, and M. Gidlund, "Modeling of the fading statistics of wireless sensor network channels in industrial environments," *IEEE Transactions on Signal Processing*, vol. 64, no. 12, pp. 3021–3034, 2016.

[100] L. Ascorti, S. Savazzi, G. Soatti, M. Nicoli, E. Sisinni, and S. Galimberti, "A wireless cloud network platform for industrial process automation: Critical data publishing and distributed sensing," *IEEE Transactions on Instrumentation and Measurement*, vol. 66, no. 4, pp. 592–603, 2017.

[101] S. M. Kim and T. He, "Freebee: Cross-technology communication via free side-channel," in *Proceedings of the 21st Annual International Conference on Mobile Computing and Networking*. ACM, 2015, pp. 317–330.

[102] T. Heer, O. Garcia-Morchon, R. Hummen, S. L. Keoh, S. S. Kumar, and K. Wehrle, "Security challenges in the ip-based internet of things," *Wireless Personal Communications*, vol. 61, no. 3, pp. 527–542, 2011.

[103] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of things (iot): A vision, architectural elements, and future directions," *Future generation comp. syst.*, vol. 29, no. 7, pp. 1645–1660, 2013.

[104] P. H. Cole and D. C. Ranasinghe, *Networked rfid Systems & Lightweight Cryptography*. Springer, 2007.

[105] H. C. Pöhls, V. Angelakis, S. Suppan, K. Fischer, G. Oikonomou, E. Z. Tragos, R. D. Rodriguez, and T. Mouroutis, "Rerum: Building a reliable iot upon privacy-and security-enabled smart objects," in *Wireless Communications and Networking Conference Workshops (WCNCW)*. IEEE, 2014, pp. 122–127.

[106] A.-R. Sadeghi, C. Wachsmann, and M. Waidner, "Security and privacy challenges in industrial internet of things," in *Proceedings of the 52nd annual design automation conference*. ACM, 2015, p. 54.

[107] A. W. Atamli and A. Martin, "Threat-based security analysis for the internet of things," in *International Workshop on Secure Internet of Things (SIoT)*. IEEE, 2014, pp. 35–43.

[108] Z.-K. Zhang, M. C. Y. Cho, C.-W. Wang, C.-K. Chen, and S. Shieh, "Iot security: ongoing challenges and research opportunities," in *IEEE 7th International Conference on Service-Oriented Computing and Applications (SOCA)*, 2014, pp. 230–234.

[109] R. Arends, R. Austein, M. Larson, D. Massey, and S. Rose, "Dns security introduction and requirements," Tech. Rep., 2005.

[110] G. Baldini, T. Peirce, M. Botterman *et al.*, "Iot governance, privacy and security issues," *Position paper, European Research Cluster on the Internet of Things*, 2015.

[111] S. Raza, "Lightweight security solutions for the internet of things," Ph.D. dissertation, Mälardalen University, Västerås, Sweden, 2013.

[112] J. H. Ziegeldorf, O. G. Morchon, and K. Wehrle, "Privacy in the internet of things: threats and challenges," *Security and Communication Networks*, vol. 7, no. 12, pp. 2728–2742, 2014.