Received: 14 March 2018 | Revised: 29 May 2019 | Accepted: 1 June 2019
DOI: 10.1002/dac.4074

RESEARCH ARTICLE

WILEY

Industrial wireless sensor and actuator networks in industry 4.0: Exploring requirements, protocols, and challenges—A MAC survey

Saleem Raza[1] | **Muhammad Faheem**[2] | **Mesut Guenes**[1]

[1] Institute for Intelligent Cooperating Systems, Otto-von-Guericke University Magdeburg, Magdeburg, Germany

[2] Department of Computer Engineering, Abdullah Gul University, Kayseri, Turkey

Correspondence
Saleem Raza, Institute for Intelligent Cooperating Systems, Otto-von-Guericke University Magdeburg, University Platz-2, Magdeburg, Germany.
Email: saleem.raza@ovgu.de

Summary

The vision to connect everyday physical objects to the Internet promises to create the Internet of Things (IoT), which is expected to integrate the diverse technologies such as sensors, actuators, radio frequency identification, communication technologies, and Internet protocols. Thus, IoT promises to transfer traditional industry to advance digital industry known as the Industry 4.0.

At the core of the Industry 4.0 are the wireless sensor networks (WSNs) and wireless sensor and actuator networks (WSANs) that led to the development of industrial wireless sensor networks (IWSNs) and industrial wireless sensor and actuator networks (IWSANs). These networks play a central role of connecting machines, parts, products, and humans and create a diverse set of new applications to support intelligent and autonomous decision making.

The IWSAN is a promising technology for numerous industrial applications because of their several potential benefits such as simple deployment, low cost, less complexity, and mobility support. However, despite such benefits, they impose several unique challenges at different layers of the protocol stack when deploying them for various monitoring and control applications in the Industry 4.0. In this article, we explore IWSAN, its applications, requirements, challenges, and solutions in the context of industrial control applications. Our main focus is on the medium access control (MAC) layer that can be exploited to satisfy such requirements. Our discussion presents extensive background study of the MAC schemes and it reviews the MAC protocols of the existing wireless standards and technologies. A number of application-specific MAC protocols developed to support industrial applications, which are not part of these standards, are also elaborated. We rationalize to what extent the existing standards and protocols help in solving such requirements as laid down by the Industry 4.0. In the end, we emphasize on existing challenges and present important future directions.

KEYWORDS

cyber-physical system, industrial wireless sensor and actuator network, Industry 4.0, Internet of Things, medium access control, wireless sensor network

1 | INTRODUCTION

A wireless sensor and actuator network (WSAN) is an extension of the wireless sensor network (WSN)[1,2] and it serves as ubiquitous infrastructure for several emerging paradigms such as the Internet of Things (IoT),[3] the Industrial IoT (IIoT),[4] the cyber-physical system (CPS),[5] and the Tactile Internet.[6,7] These technological advances put together sensing, computing, and control along with wireless networking and information and communication technologies (ICT) to revolutionize the fourth industrial revolution, the Industry 4.0.[8] The Industry 4.0 promises to make existing factories smart enough for producing high-quality products with lower manufacturing costs. Therefore, it has exerted a considerable impact on controlling and realizing the physical production processes in a real-time to achieve greater productivity, worldwide.[9] It will enable a variety of desired quality level products with a high degree of freedom at a constant price which will be available for customers anytime and anywhere in the world. Currently, all manufacturers demand an autonomous interaction and highly stable local and global interconnectivity among various systems and subsystems in their factories to overcome the growing interconnectivity issues of operators, machines, and products.[10] Presently, all devices within the factories are connected through wired or wireless communication technologies working over traditional industrial protocols for providing stable networking. However, the wireless communication technologies, because of their number of advantages, can play an important role to streamline management of operations in Industry 4.0. [10]

In particular, the use of WSNs and WSANs in industries has gotten increased attention because of low cost, simple deployment, and flexibility reasons and has given rise to industrial WSNs (IWSNs) and industrial WSANs (IWSANs). These networks target to decentralize the decision-making process so as to attain autonomous operation and involve less human interaction. Such autonomous aspect is of high significance for diverse industrial applications to support smart systems and processes. This in turn increases the production reliability and economic benefits. However, the unique nature of the industrial environment due to equipment noise, heat, dust, fading, multipath effects, and electromagnetic interference[11] bring a number of challenges to these wireless networks at different layers of the protocol stack. As a result, the performance of quality of service (QoS)-aware data delivery for various IWSN-based industrial applications can be hampered. To eliminate such challenges, over the last few years, we witness diverse low-power wireless standards and technologies to address those challenges.[12] Primarily, the IEEE 802.15.4[13] standard has undergone significant improvements to meet the requirement of industrial applications. This is the reason that most of the wireless standards and solutions in the market such as ZigBee,[14] THREAD,[15] Z-WAVE,[16] 6LoWPAN,[17] LoRa,[18] WirelessHART,[19] International Society of Automation (ISA),[20] and WIA-PA[21] are based on this standard. All these developments have accelerated the adoption of IWSN and IWSAN in safety and time-critical process control and automation applications.[22-24] Particularly, an enormous focus has been devoted in the design and development of efficient medium access control (MAC) protocols to accomplish an improved network performance while satisfying the application QoS. Since, MAC directly impacts multitude of performance metrics such as reliability, scalability, low latency, energy efficiency, and security.

In this paper, we present a comprehensive discussion and review on the IWSANs in the context of Industry 4.0 mainly focusing on their MAC layer schemes. We primarily emphasize on industrial applications, requirements, and challenges in the context of wireless sensor nodes. We present and compare various MAC protocols and mechanisms of existing wireless standards and technologies such as WirelessHART and ISA 100.11a. Finally, we address key research challenges and elucidate future directions. The key contributions of the paper can be summarized as follows:

- discuss the evolution of Industry 4.0 and present communication technologies that play crucial role towards achieving the Industry 4.0 vision.
- Discuss benefits of wireless technology in industry and highlight its impairments and challenges compared with wire counterpart. We give an overview of the open systems interconnection (OSI) protocol stack with reference to WSN perspective, which is a simplified version of OSI model.
- Explore WSNs in the context of industrial applications, especially the networked control system (NCS). Discuss the architecture of IWSN and IWSAN in general with reference to industries and particularly discuss the characteristics of IWSAN.
- Highlight differences between WSN and WSAN and rationalize how such differences impose additional constraints on MAC protocol design.
- Present industrial application categories and classes and discuss sensitivity, criticality, and importance of the traffic under each category. Discuss major impositions laid down by each category and address how important it is to fulfill them. In case of failure to comply with these impositions how the application QoS parameters are affected.
- Analyse the characteristics and influence of the MAC layer and how it can effectively be exploited to solve the issues pertaining to IWSN and IWSAN.

- Review existing wireless standards and technologies with particular focus on their MAC schemes. We explain how their MAC design choice helps solve the challenges that previously remained unsolved.
- Give an overview of the important industrial standards especially WirelessHART, ISA100.11a, and WIA-PA and their MAC schemes. In addition, other nonstandard protocols that have been developed to support IWSAN applications are part of our discussion. We critically discuss their operation and highlight their advantages and disadvantages.
- Determine important challenges that should be taken into account while proposing new protocols for IWSAN. We emphasize, to what degree, recent protocols and standards solve these challenges and what further improvements are needed.
- Finally, we elucidate future directions that enlighten what research needs to be conducted to meet the requirements of IWSAN for the Industry 4.0.

The remainder of the paper is organized as follows. Section 3 focuses on the Industry 4.0 and presents the key communication technologies to be used in industries. Section 3.1 describes the benefits of wireless technology and challenges associated with the use of wireless medium. Section 5 explains WSN and highlights the role of WSN in the Industry 4.0. Section 5.1 explains the general architecture of IWSN and IWSAN and presents their distinctive characteristics. It highlights the unique differences between WSN and WSAN. Important applications and requirements of IWSAN are discussed in Section 6. Section 7 explains the MAC layer, its characteristics and influence, and gives the classification of MAC schemes. Section 8 covers the MAC schemes employed by existing wireless standards and technologies. Section 9 provides details on the nonstandard MAC protocols proposed for IWSAN applications. Section 10 presents key challenges and future directions. Finally, a conclusion is drawn in Section 11.

2 | KEY DRIVING TECHNOLOGIES FOR INDUSTRY 4.0

The IoT focuses on undertaking common objects and turning them into connected smart objects with the help of sensing, computing, and communication capabilities.[3] IoT interconnects billions and even trillions of daily objects to the Internet to construct a networked feedback loop of sensing, transmitting, and communicating with one another so as to realize a common goal.[4] In this way, its promises to transform and improve home, business, and industrial applications and move forward to a more sustainable, safe, and secure society. The recent proliferation of IoT in industrial domain has been termed as the IIoT, which focuses on machine-to-machine (M2M) and industrial communication technologies and focuses mainly on the transfer and control of mission-critical applications.[25] Whereas, the CPS are considered to be the integral parts of the IIoT, which focus more on the smart factory, industrial automation, actuators, etc. [5]

All those terms are closely related and serve as the key drivers for the fourth industrial revolution coined as the Industry 4.0. The Industry 4.0 encompasses all above technologies that are expected to play a pivotal role in promoting manufacturing to be more digital, information-led, customized, and green. It involves humans, machines, networking, physical process, product, machines, and embedded systems with interactive software such as sensors, actuators, radio frequency identification, intelligent controllers, computers, laptops, tablets, mobile devices, smartphones, and several others. [26,27] The main ideas of the term Industry 4.0 were first discussed in 2011 at the Hannover Fair as a high-tech strategy for 2020 in Germany.[28] Similar ideas have been discussed in other industrial countries, such as "Internet +" in China, "The Fourth Industrial Revolution" in Korea, "Factories of the Future" in Europe, and "Industrial Internet" in the United States.[29,30] Despite the great interest in the concept of Industry 4.0, it has become a hot spot for most global industries in recent years. The charm of Industry 4.0 paradigm is twofold. First, it promises huge economic impact, substantially increased operational effectiveness, and the development of completely innovative products, services, and business models. Second, it offers a number of great opportunities for research institutes and corporations to actively shape the future.

However, all these technology drivers are incomplete without the core foundation of IWSN and IWSAN, as the sensing and actuation are integral aspects of them. Thus, ensuring reliable, scalable, energy efficient, safe, and secure communication among these networks is crucially important. Only then can the QoS aspects of the industrial applications be guaranteed. However, to meet all these performance goals puts a great deal of challenges that need to be addressed. First and foremost, the issues associated with wireless technology are dynamic channel conditions, link quality variations, fading, etc. Second, issues pertaining to ensuring deterministic and low latency communication. The third challenge, which is to ensure low-energy operation is of vital significance as the sensor nodes have constrained resources. Therefore, more research efforts are required to overcome these challenges so as to ensure an acceptable network performance and accelerate adoption of IWSAN.

3 | WIRELESS TECHNOLOGIES IN IN INDUSTRIAL APPLICATIONS

In this Section, we briefly discuss how industrial applications can benefit from the wireless technology compared with wired technology. The discussion considers the important challenges induced by the wireless technology and how they impact different aspects of the industrial applications.

3.1 | Benefits

- Cost reduction. The main operational expenditure and capital expenditure in industries are of wiring, whose installation and maintenance incur huge costs. Using wireless solutions greatly reduces these costs. They have appealing benefits, for instance, rapid installation, easy maintenance, easy system reconfigurations, etc. In this way, they not only contribute to cost reduction but also save time.
- Flexible architecture/design. Wireless technologies offer a great deal of flexibility compared with wired solutions. There is no additional expenditure involved due to addition and removal of wireless sensor nodes and other necessary wireless equipment. Certain processes in industries such as robots and rotating equipments are severely hindered by hard and fixed locations of wired solutions, but wireless solutions can flexibly handle such processes. In addition, wired solutions are not appropriate to be deployed in dangerous areas because of surrounding temperatures, whereas wireless solutions can flexibly work in such areas.[31]
- Safe procedures. Reconfiguration and maintenance of processes in dangerous areas are carried by humans, which can endanger their lives because of potential hazards. Wireless solutions make it safer by remotely reconfiguring and maintaining processes and systems, avoiding humans to be involved in hazardous locations. Moreover, mechanical failures of connectors is a common problem in industries, which affects the reliability and causes downtime of industrial applications. Wireless solutions are free from the wear and tear kind of failures, which make them more safe and less prone to failures.[32]

3.2 | Challenges

Despite the offered benefits of wireless technologies, they simultaneously induce several nontrivial challenges that require serious efforts to deal with.[33] The imperfect and error-prone wireless medium results in packet losses and variable communication delays. Wired networks also exhibit such losses but in case of wireless networks, they are more amplified because of varying channel conditions, limited spectrum, multipath propagation, and fading.[34] Besides, an important issue is to efficiently utilize and provide access to the shared wireless medium, which is handled by the MAC sublayer, which is a part of the data link layer. An inefficient MAC scheme can actually waste scarce communication resources. Below, we discuss important challenges induced by wireless medium.

- Packet losses. Packet losses are common in the wireless medium due to various channel impairments like multipath fading, collisions, and weak channel gains.[35] Buffer overflow causes congestion, which renders packets to be lost in transit. Long transmission time results in packet reordering, which causes packet dropouts.
- Variable communication delay. Network conditions invariably induce random delays and cause an uncertain amount of time for data to reach the destination. Data have to be sampled, encoded, and transmitted. The same have to be decoded on a receiver side, which adds delay.[36,37] For WSNs applications, the packets transmitted are time stamped, which helps the receiver get an estimate of the delay and take appropriate measures. For instance, under contention-based MAC schemes (see Section 7), main causes of variability in delay arise when multiple nodes try to access same wireless link simultaneously, which results in collision and then each node has to wait a random amount of time before reaccessing the medium. This reaccessing of the medium increases the delay. Link quality between nodes also affects delay to increase. With poor link quality, retransmissions are more frequent, which increase delay as well as energy consumption. Delay is a crucial performance indicator whose variability should be as minimum as possible. An adequate upper bound for delay should be ensured so that negative impacts on application QoS can be avoided.
- Data rate. Limited bandwidth of the channel imposes the constraint on the number of devices sharing the medium, which may impact the network capacity.[36,38] The packet size and its overhead influence the data rate of the communication network, thus, an efficient protocol scheme may help minimize the overhead. Since WSNs have low data rates, this may be a constraint for certain industrial applications.

All aforementioned imperfections of the wireless medium may cause performance degradation for IWSN applications. Therefore, efficient protocols are required to compensate for these losses and minimize adverse affects.

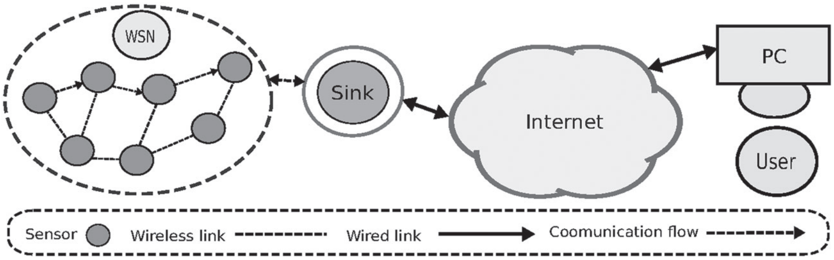


FIGURE 1 A general wireless sensor network (WSN) deployment scenario

4 | ROLE OF WSN IN INDUSTRY 4.0

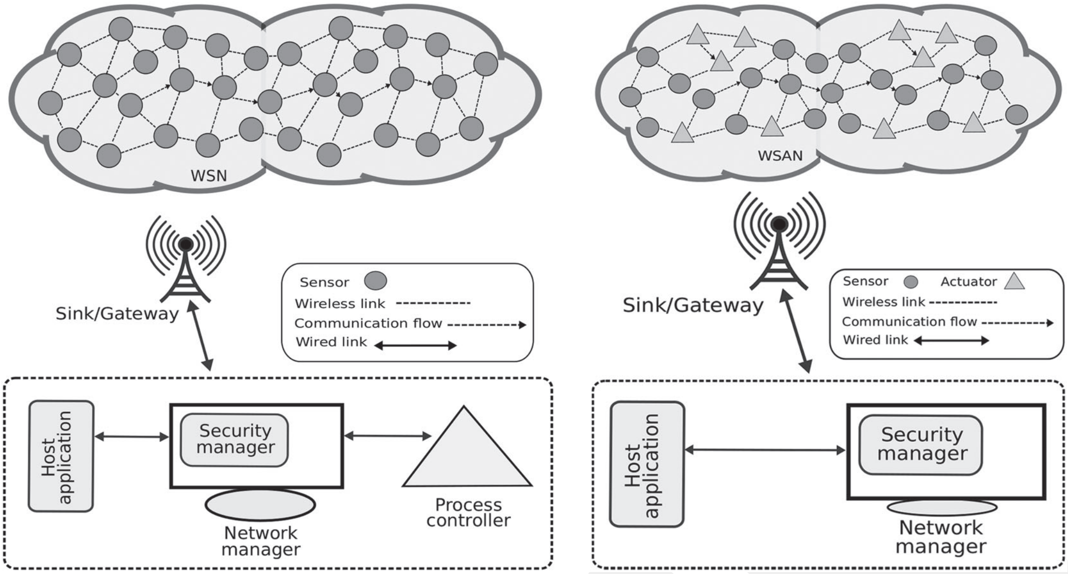
At the core of Industry 4.0 are the WSNs, which consists of low-cost multifunctional nodes (also called motes) that, along with sensing, have the capabilities of processing and communication.[39] These small and low-cost sensor nodes have embedded processors and transceivers to communicate wireless over short distances.[40-42] They are densely deployed in an area of interest to collect sensory data (temperature, pressure, or vibration, etc.) by collaboratively coordinating and exchanging information by forming wireless ad hoc networks. The resulting networks are known as WSNs as shown in Figure 1. Sensor nodes are constrained in terms of power, processing, and communication because of their small size and use of batteries.

A unique feature of WSNs is their in-network processing[39] attribute, whereby sensor nodes do not send raw sensed data directly to the gateway but instead fuse it locally to make it more consequential to save extensive communication costs. Because of their unique attributes, their application domain is diverse and they are now ubiquitous components of smart environments. Their diverse application domain covers military,[43,44] surveillance,[45,46] home automation,[47,48] smart city,[49,50] patient health monitoring,[51-53] etc. In patient health care monitoring scenarios, WSNs are used in tele-health applications.[54] For example, to monitor chronically ill patients and to regularly check their different parameters like glucose level, heartbeat, and send that information wirelessly to a remotely located doctor for further diagnosis. WSNs are also used to assist elderly and disabled people in their daily routine tasks. Over the past few decades, they have undergone large deployments in diverse applications, including transportation,[55,56] agriculture,[57] industrial process automation and control,[58-60] and supply chain management.[61] Because of their ubiquitous presence and considering potential benefits leveraged by these networks—such as simple deployment, cheap installation cost, no wiring cost, less complexity, and mobility—they are increasingly used in industrial applications,[58] which have resulted into IWSNs.

WSNs can be deployed in industrial environment such as industrial monitoring,[60] process automation and control,[62] and emergency and safety[63] applications. In process automation and control applications, certain tasks may require acting nodes known as actuators that have the capability to autonomously act on the physical environment based on the sensed measurements. Over the last decade, sensors and actuators have been used together to perform autonomous tasks. The integration of industrial sensors and actuators has resulted into IWSANs. For example, in feedback-based chemical process automation and control, sensors measure the temperature; if the temperature crosses a certain threshold value, they inform actuators (eg, connected to a valve) to reduce the temperature to a desired value so that the process remains in a stable state. Such applications impose strict constraints on reliability and low latency[64] because measurements of the sensors have to reach the actuator timely and reliably so that the act of controlling valve is performed on time.

5 | INDUSTRIAL WIRELESS SENSOR NETWORK

Compared with early resource constrained sensor nodes, today's sensor nodes—because of recent improvements in technology—have more processing power, memory, and prolonged battery life.[65] This has enabled them to be used in industrial applications and resulted into IWSN.[59] IWSN makes processes independent and autonomous, especially in harsh areas to obtain sensory, actuation, and control information.[31] Figure 2A depicts the general architecture of IWSN that consists of WSN field, network manager-cum-security manager, process controller, and host application management. The sensor nodes in WSN field sense the process variables (eg, temperature, pressure, etc.) and transmit it to the sink or gateway. The sink then forwards it to the process controller whose job is to control the process variable under certain desired value. The sink is responsible to manage the sensor network and is managed and controlled by the host application management. The network-cum-security manager is responsible to look after the over all network along with ensuring security against attacks. The arrows in Figure 2A indicate the direction of the communication flow where sensor data is transmitted to the sink in a multihop fashion via intermediate sensor nodes. IWSN has the potential to improve



(A) General architecture of the IWSN showing sensor network field connectd through sink to controller, network manager cum security manager and application console.

(B) General architecture of the IWSAN showing sensor actuator network field along with the sink which is connected to the controller, network manager, and application console.

FIGURE 2 General architecture of the industrial wireless sensor network (IWSN) and industrial wireless sensor and actuator network (IWSAN), depicting IWSN and IWSAN field together with sink. The sink is then wire-connected to the rest of the industrial network (dashed line)

production processes and quality of products without compromising the QoS. Thus, making the concept of smart factory a reality. In most of the industrial applications, along with sensing, actuation and control are also imperative aspects. In these applications, sensors sense data and actuators act on the data based on certain control decisions made by the process controller. Below, we describe more about the sensor and actuator networks.

5.1 | Industrial wireless sensor and actuator network

Because actuation is an integral part of the industrial processes and systems, therefore, the increasing trend is to integrate sensors and process controller (actuators or actors) to perform sensing and actuating tasks, ie, sensor nodes have been equipped with actuators. Succinctly, the actuators are transducers that have the capability to convert an electrical signal into a physical action, a typical actuator example includes a valve that controls flow of the water or gas in a tank. [1]

Actuators are also called as actors* in the context of WSN. Here, the actors not only act on the physical environment but also possess networking capabilities such as receive, transmit, process, and relay data. For example, a robot working in the industries may act on the physical environment by means of various motors and servo-motors (actuators). However, from a networking perspective, the robot may be considered a single networking entity, which we call as actor.[66] Thus, an actor may involve more than one actuators, which means they encompass heterogeneous devices. This hybrid combination of sensors and actuators has developed a new class of research known as WSAN.[1] Figure 2B shows WSAN in industries also known as IWSAN. Here, WSAN is a distributed sensor/actuator field where the sensors have direct communication with the actuators and the actuators can also communicate among themselves. Hence, unlike WSN, where sensors always communicate sensed data to the sink, WSAN involves sensor-to-actor and actor-to-actor data communications via single-hop or multihop transmissions.

WSAN has the capability to perform distributed sensing, data fusion, collaboratively making decisions, and performing appropriate actions on physical environment.[2] For example, sensing water level or flow and sending data to the actuator, and actuator controls level or flow of water. In this way, the information that is sensed can be efficiently utilized to perform appropriate actions. A distinct characteristic of actuators is that they are usually rich in resources like computational, communication, and battery power. In some cases, actuators may also perform sensing tasks. However, compared with normal sensor nodes, they impose strict constraints on reliability, predictability, and availability.[59,60] Since actuators have

---

*Throughout this text, we use the terms actuator and actor interchangeably.

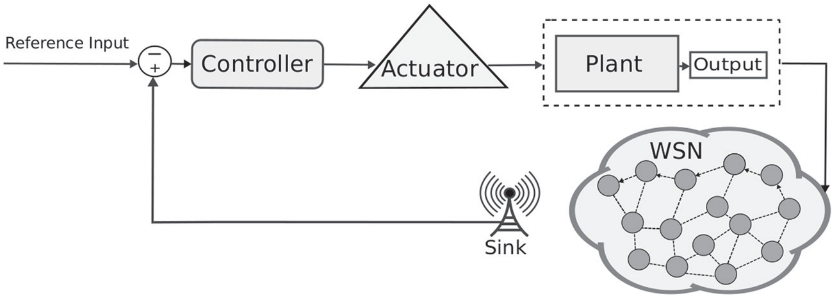


FIGURE 3 Wireless closed-loop control realized through wireless sensor network (WSN). Sensor measurements are sent to the controller through the gateway, which is wire-connected to controller

TABLE 1 Comparison of WSNs and WSANs in nutshell

WSN	WSAN
Resource constrained nodes	Resource resource rich nodes like actuators
Short distance communication	Long distance communication due to actuators
Flexible in terms of real time requirements	Strict real time requirements
Not complex coordination	Complex coordination among sensors & actuators
Homogeneous environment	Heterogeneous environment

Abbreviations: WSAN, wireless sensor and actuator network; WSN, wireless sensor network.

rich capabilities, they are not as densely deployed as sensor nodes. A few actuator nodes would suffice with different coverage requirements. Additionally, the sink or gateway is required to monitor the overall network.

One of the most promising applications of IWSANs is in the industrial NCS, including closed-loop or feedback control system. Figure 3 shows IWSANs in a typical industrial closed-loop control application. Here, the whole control loop is realized through WSN. Another interesting application of WSAN is the smart home, where based on some user prescribed settings, sensors send data to appropriate actuators to perform an action. For instance, to turn on and off light bulbs or control air conditioning based on settings already prescribed. WSAN is a promising class of research, where not only the data is sensed and communicated but is also acted upon, which is an interesting feature.

5.2 | Characteristics of WSAN

Generally, actuation activity is a bit complex compared with the sensing. Besides, depending on the application, there may be an immediate response to a sensor input required, which further imposes certain real-time constraints. Therefore, with WSAN, the requirement of real-time communication comes into play. WSANs are characterized by some of the following unique features.

- Real-time guarantee. Real-time requirement is interchangeably dealt with latency and delay bound, ie, there are strict timing constraints involved between sensing and acting. This means that as soon as data is sensed, it should timely trigger actuators to act. If the required data encounters latency and actuation command is performed late, it makes data less effective, meaning sensing data must be valid at the time of acting.[2] For example, in a fire detection and extinguishing application, once the sensors sense fire, it requires timely action from actuators to trigger fire extinguishers so that fire can be controlled before it gets further deteriorated. Table 1 highlights the comparison between WSN and WSAN in a nutshell.
- Reliable coordination. An interesting feature of WSAN is that sensors not only communicate among themselves but also with actuators. Thus, there are sensors-to-actuator and actuator-to-actuator coordinations involved.[2] These coordinations involve selection of the suitable actor to perform the action based on different metrics such as its available energy, coverage, distance, location, etc. These coordinations are of fundamental importance to maintain the required reliability, self-organization, and QoS of the network, but at the same time, they impose new challenges on networking to provide robust and delay tolerant protocols and solutions.
- Traffic differentiation. With the presence of resource-constrained sensors and resource-rich devices like actuators, the environment is heterogeneous. Therefore, efficient resource allocation and utilization techniques need to be developed. Energy efficiency for sensor nodes is a big concern but for actuators is of less concern. Moreover, actuating messages are more delay sensitive than normal sensor measurements, so message priority differs in both. Therefore, heterogeneity needs to be exploited intelligently in protocol design so that application QoS requirements and constrained resources of the sensors are not at stack.

6 | IWSAN APPLICATIONS AND REQUIREMENTS

Industrial domain encompasses applications, ranging from monitoring and control to safety or emergency, process automation, factory automation, closed-loop control, predictive maintenance, etc. Different applications require different priorities. Moreover, frequent streaming updates related to configuration changes, alarms, and command instructions keep refreshing. On the basis of the criticality of data, six application categories are defined by ISA[67] as given in Table 2.[60,68] Next, we give a brief discussion of each application category along with its traffic type.

6.1 | IWSAN applications

In this section, we discuss different application categories in the industry and present the nature of the traffic generated in each category. We emphasize how these categories vary in terms of criticality, reliability, timeliness, and importance of data. Subsequent description talks more about each category in detail.

- Safety systems. These systems are directly related to emergency actions. They are always critical in nature and require immediate action to be taken, ie, real-time communication is desired. These systems are extremely delay sensitive and require low latency and high reliability. But in terms of bandwidth requirements, they tend to have moderate bandwidth.
- Control systems. The major part of the industrial applications requires control operations. Several control systems exist such as closed-loop control systems,[69] open-loop control systems, process control systems, etc. Generally, closed-loop control systems monitor processes and act accordingly as per the control decision. These systems are generally autonomous and do not involve humans in the loop. Examples of such systems include process control systems and factory automation systems. Open-loop control systems do not have feedback and require humans in the loop, ie, adjustments are done by humans. Each control system imposes different delay requirements, for example, closed-loop control data is more critical than open-loop control data. Specially processed control systems can tolerate delay greater than 100 ms, but on the the other hand, factory automation requires even less delay (2-50 ms),[60] ie, robot coordination involvements.
- Alerting systems. These systems are characterized by the features, such as regular events/alerts, as a result of continuous monitoring. They indicate short-term operational consequences at different stages of processes or system.
- Predictive maintenance and automatic fault detection. This is useful in industries as it ensures the prediction of a machine failure before it actually occurs.[70,71] This is basically driven by the condition monitoring together with possible automatic maintenance utilizing advanced algorithms.[72] This is a crucial challenge because the unexpected shutdown of machines or equipment lead to unscheduled downtime, which incurs huge losses. Therefore, a reliable sensor and actuator network is required to precisely predict the machine failure. The collaborative nature of sensors and actuators networks can jointly predict detection of faults and help avoid worst-case situations.
- Monitoring systems. This includes monitoring process variables, equipment condition monitoring, and structural health monitoring, etc. The general goal of monitoring is to continuously gather data from an area of interest for long

TABLE 2 Different classes of applications as defined by ISA,[67] the traffic categories are listed according to traffic priority where 0 being the highest priority traffic and 5 being the lowest priority traffic[68]

Category	Class	Application	Latency	Description
Safety	0	Emergency action	10 ms (deterministic)	Always critical, eg, instrumented protective systems/safeguarding systems
Control	1	Closed-loop regulatory control	10 ms to 100 ms	Often critical, eg, regular control loop control
	2	Closed-loop supervisory control		Usually noncritical , eg, set point manipulation for control system optimization
	3	Open-loop control		Human in loop, eg, manual human actions on alerts
Monitoring	4	Alerting		Short-term operational consequence, eg, event-based maintenance
	5	Logging and downloading/uploading	100 ms on average	No immediate operational consequence, eg, history collection, sequence-of-events, preventive maintenance

durations, analyse the data, and use this data to make better decisions so as to derive certain conclusions. These systems cover almost every aspect of the industrial applications.

6.2 | IWSAN requirements

This section elaborates the requirements of IWSAN applications, their characteristics and interdependencies in the context of MAC protocol design.

- Reliability. The wireless medium is unreliable and link quality varies over time. It is assumed that bidirectional links do not have the same link quality in both directions. Poor link quality can deteriorate transmission and cause latency, which can deteriorate control decisions to be taken on time, which, in turn, can lead to system failures and economic losses.[73] The reliability can be treated at different levels. For example, it can be a function of energy efficiency, ie, the network lifetime should be adequate enough to perform reliably over that period. Reliability can be characterized in terms of packet reception rate, ie, packet reception rate should be above a certain threshold to guarantee a certain level of reliability in which processes and systems work without further degradation.
- Packet priority and heterogeneity. Industrial domain is heterogeneous, different types of packets are generated like sensing measurements, controlling commands, actuation tasks,[74] etc. Each of the traffic has a different priority to be treated. Therefore, adding packet priority ensures a certain degree of timely action performance. Some actions require immediate execution, while others can tolerate a certain level of flexibility for execution. For example, in closed-loop control systems, controlling and actuation commands are more critical than sensor data. So, a level of priority difference should be embedded in protocol design so that in case of faults, system should respond appropriately.
- Energy efficiency and power consumption. Since for battery-powered sensor nodes, it is almost impossible to replace battery especially in inaccessible areas in industries. Nevertheless, energy efficiency is also a major concern as reliability and latency. Improving energy efficiency also adds value to reliability in the same manner as reliability in terms of low latency and packet reception rate. However, reliability and low latency demands may cause significant energy consumption.[75] Therefore, careful tradeoffs need to be taken care of under existing metrics tradeoffs' complexity. Analytical or experimental evaluation to analyse the tradeoffs will lead us to develop robust and flexible protocols.
- Adaptation. Often the traffic requirements of control applications change dynamically with respect to different states of the process controller. In addition, varying wireless medium and network topology changes may impose further requirements. To cope with such dynamic traffic behavior, communication protocol must adapt its parameters as per the requirements of control application as well as wireless medium.
- Scalability. Scalability refers to the ability of a system to scale well or provide a high degree of flexibility.[76] It supports adaptivity to changes with respect to addition and removal of nodes or functionality without degrading its existing performance. Generally, IWSAN may require hundreds or even thousands of nodes, therefore, communication protocols need to be scalable to comply with such requirements. However, the development of scalable MAC protocols is a nontrivial task and imposes a huge challenge. Existing wireless standards such as WirtelessHART and ISA100.11a largely utilize time division multiple access (TDMA)-based protocols, which impose strict constraint on the number of participating nodes and at the same time satisfy application QoS requirements. Therefore, in order to achieve better performance, IWSANs require protocols that can support scalability at different layers of the protocol stack.
- Multihop communication. Industrial applications usually undertake large-scale network deployments because of bigger plants spanning over a large area. Thus, a large number of sensor nodes are deployed at different floors and locations. In this case, sensor nodes need to transmit not only their own data but also relay data of nodes which are multiple hops away from the sink. Therefore, establishing a multihop communication is inherently part of such scenarios. This allows further flexibility of adding new nodes in the existing network in case of structural changes in industrial plants.[77] It also adds redundancy. In case of primary communication path failure, nodes can utilize alternative path to reach the sink. However, this also imposes challenges of how to select a particular relay node if there are multiple relay nodes available so as not to overload a particular path and ensure timely delivery of data.

7 | MAC LAYER CHARACTERISTICS AND INFLUENCE

Because of the broadcast nature of wireless medium, two nodes transmitting within their effective communication range can severely interfere with each others' transmission, resulting in collisions and wastage of the resources.[78] MAC is a part of the data link layer within simplified communication stack of WSN as shown in Figure 4. It specifically administers

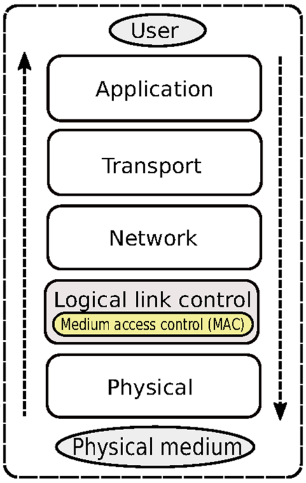


FIGURE 4 Simplified communication stack for wireless sensor network (WSN)

access to the shared wireless medium, avoids collisions, and manages resources. Depending on application requirements, it coordinates a communication schedule among nodes. MAC influences many application performance metrics such as latency, reliability, energy efficiency, and security. For example, by intelligently reducing collisions, it can control latency and energy consumption. Several MAC protocols have been developed for conventional wireless networks,[79,80] but none of them suits low-power requirements of WSNs because all those protocols were designed without taking into account the energy constraints of sensor nodes. Several protocols tailored to traditional WSNs[78,81] are not suitable for WSANs, because of the complex coordination among sensors and actuators. On the basis of application classification given in Section 6, closed-loop control systems often require critical data delivery with low latency and high reliability. This urges to design MAC protocols that comply with these performance metrics so as to maintain the application QoS parameters.

The performance requirements for traditional wireless networks are latency, throughput, fairness, delay, etc. However, because of the unique properties of WSN, such as resource constraints, distributed nature and different traffic characteristics posed unique challenges. For WSN, the requirement of energy efficiency is of utmost importance, which ensures an adequate network lifetime. Therefore, for IWSAN, the requirements of reliability and latency are of equal importance as of energy efficiency.

7.1 | State of the art MAC schemes

MAC protocol development has been an active area of research. A large number of MAC protocols exists in literature and can be found in Bachir et al, Zhao et al, and Suriyachai et al.[78,81,82] Each application imposes different requirements for MAC, therefore, in response to fulfilling those requirements, several protocols emerged. Fundamentally, each protocol, with its different design, tries to define a way to access the medium and achieve application-specific requirements. Generally, MAC schemes can be classified into three broad categories known as *schedule based*, *contention based*, and *hybrid schemes*[83,84] as depicted in Figure 5. These schemes fundamentally utilize two major multiple access approaches: carrier-sense multiple access (CSMA) and TDMA. Other known approaches are code division multiple access (CDMA),[85-87] frequency division multiple access (FDMA),[88] orthogonal frequency division multiple access (OFDMA),[89] and space division multiple access (SDMA). A brief explanation of some of these categories is presented as follows.

7.1.1 | Schedule-based schemes

These are also called fixed assignment or reservation based schemes. Each node is assigned available resources for a fixed duration of time which are used exclusively by the node. The protocols in this class are TDMA, FDMA, and CDMA as described below.

- TDMA. Time is divided among sensor nodes and each node gets a specific portion of time, in the form of *time slots*, to access the medium and transmit data. Most of these schemes follow a superframe structure, which contains time slots for each network node and keeps repeating for a defined duration of time. For a successful TDMA slot assignment, synchronization among nodes is crucially important. A simple TDMA scheme with superframe is shown in Figure 6.[31]
- FDMA and CDMA. In FDMA, the available frequency spectrum is divided into a number of subchannels. Each node is allocated a specific subchannel. In CDMA, the signal is sent via spread spectrum technology and a special encoding scheme is used to allow multiple signals through the same channel. Although FDMA and CDMA are two important

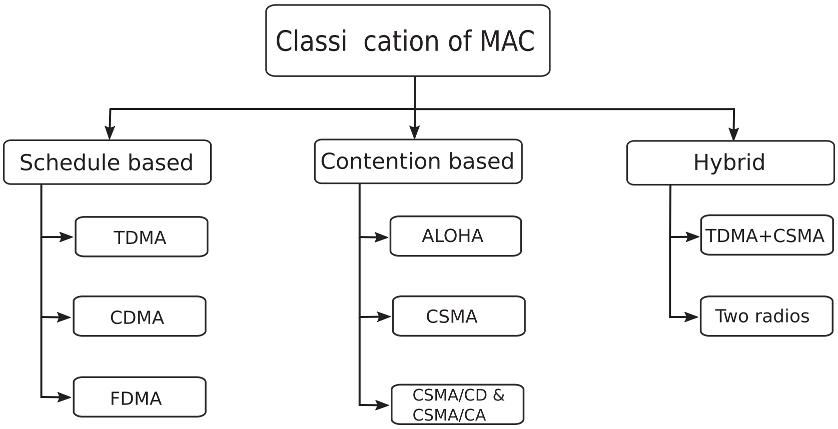


FIGURE 5 Classification of medium access control (MAC) protocols

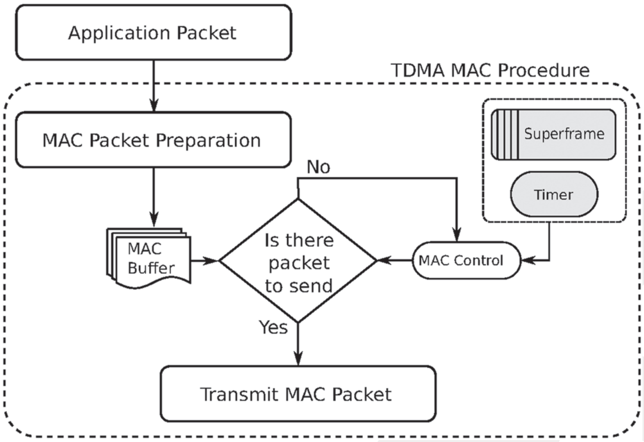


FIGURE 6 A simple time division multiple access (TDMA) medium access control (MAC) procedure through superframe representation

medium access schemes, they are generally less suitable for WSN because of their complex design and extremely high energy consumption.[83,84]

There are several advantages of schedule-based schemes like collision-free communication, inherent duty cycle, overhearing, and idle listening avoidance.[90] All these aspects are contributing to save energy. These schemes tend to be more predictable and can offer deterministic end-to-end delay. However, with the increasing number of nodes, the queuing delay is much higher because nodes have to wait for their dedicated time slots to access the medium. Synchronization is a big concern and causes high complexity in these schemes, which generate extra traffic because of control packet exchange. Generally, these schemes are less flexible and scalable, they are less suitable where dense deployment of WSN is a prime requirement.

7.1.2 | Contention-based schemes

In this approach, nodes compete with one another to gain access to the medium and transmit data. They access the channel by first sensing it before transmission. The act of channel sensing is performed independently of one another. The channel is allocated for the duration required to communicate data in hand. Once data communication has been completed, the channels are freed. Protocols under this class are:

- Additive Link On-Line Hawaii System (ALOHA). The pioneering protocol in this class is the ALOHA[91] protocol, in which each node initiates transmission whenever it has data regardless of the other nodes' transmission at the same time and results into collisions. Another variant of ALOHA is the slotted ALOHA, which is more efficient than pure ALOHA, in which nodes initiate transmission only at the beginning of the slot which decreases the chance of collisions.
- CSMA. It allows nodes to be more modest in terms of accessing channel. Nodes first sense the channel to determine if any other transmission is already in progress (channel busy) if so, they have to wait a random amount of time and try again later. However, if a channel is sensed free, they immediately proceed with their transmission. A simple CSMA scheme is depicted in Figure 7. There are different variants of CSMA scheme like *nonpersistent* CSMA, *persistent* CSMA, *p-persistent* CSMA, and *I-persistent* CSMA. Each of these variants tries to minimize collisions and achieve better

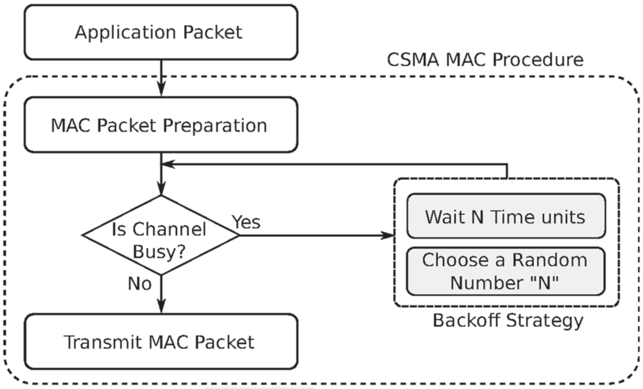


FIGURE 7 A simple carrier-sense multiple access (CSMA) medium access control (MAC) scheme procedure

TABLE 3 Different medium access control (MAC) schemes with their features, strengths, and limitations

MAC Schemes Metrics Comparison					
Metric	**Pure-ALOHA**	**CSMA**	**TDMA**	**FDMA**	**CDMA**
Collision probability	✓	✓	✗	✗	✗
Bit rate flexibility	✗	✗	✓	✗	✓
Synchronization overhead	✗	✗	✓	✓	✗
Energy efficiency	✗	✗	✓	✗	✗

performance by modifying some parameters. Other variants are CSMA/collision detection (CSMA/CD) and CSMA/collision avoidance (CSMA/CA).

The consequential benefits of contention-based schemes are that they are adaptive towards change in network conditions and adjust their performance according to traffic loads.[92] They are more flexible to topology changes and scalable to node density compared with the schedule-based approach. Because of independent channel accessing decisions, they do not require extra message exchange overhead. Their main drawback is of energy inefficiency, which is caused because of collisions, idle listening, and unfair load distribution. With increased node density, the probability of collisions increases, which causes retransmissions and limits throughput and wastes energy. The protocols in this class can follow both centralized control and distributed control approaches similar to schedule-based schemes. [39,83]

7.1.3 | Hybrid schemes

These schemes combine both schedule-based and contention-based techniques to offer potential improvements. They usually have two modes, one utilizing schedule-based and other contention-based approaches. They jointly maintain switching between the two as per the requirements. Certain examples of protocols based on hybrid scheme are Z-MAC,[93] ER-MAC,[94] and a hybrid MAC protocol for WSN.[95] Table 3 shows the comparison among all the aforementioned MAC schemes based on different performance metrics highlighting their strengths and limitations.

8 | EXISTING WIRELESS STANDARDS AND SOLUTIONS

In this section, we give a detailed overview of the IEEE 802.15.4[96] standard which is widely known as low-power wireless standard for WSN. We also present different low-power standards based on IEEE 802.15.4. Subsequently, we discuss three industrial standards: WirelessHART,[19] ISA100.11a,[20] and WIA-PA.[21] The discussion mainly focuses on their PHY and MAC layers.

8.1 | IEEE 802.15.4

The IEEE 802.15.4 standard was developed in 2003.[96] It was designed targeting low-rate wireless personal area network (LR-WPAN) and offers simple, low-cost, short-range, and low-energy characteristics. The standard mainly defines PHY layer and MAC sublayer specifications. It supports different topologies such as star, peer-to-peer, and mesh as shown in Figure 8. The standard introduces two types of devices on the MAC, *full-function devices* (FFD) and *reduced-function device* (RFD). FFDs are more powerful and support three functional modes; they can serve as personal area network (PAN) coordinator, a coordinator only, or an end device. An FFD can form a PAN after obtaining a valid PAN identifier, it can talk to other FFDs and RFDs. Whereas, RFDs have constrained resources—they can only talk to a single

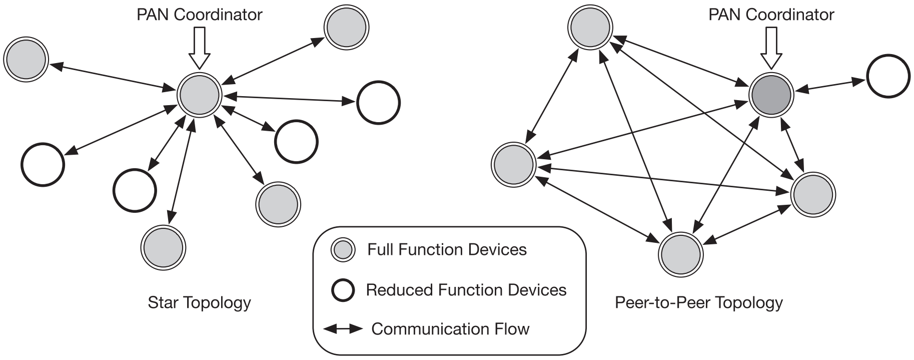


FIGURE 8 Different network topologies supported by the IEEE 802.15.4 standard

TABLE 4 Different frequency bands supported by the IEEE 802.15.4 standard

	2.4 GHz	**915 MHz**	**868 MHz**
Allowed region	Worldwide	America	Europe
Data rate	250 kbps	40 kbps	20 kbps
No. of channels	16	10	1
Modulation	O-QPSK	BPSK	BPSK

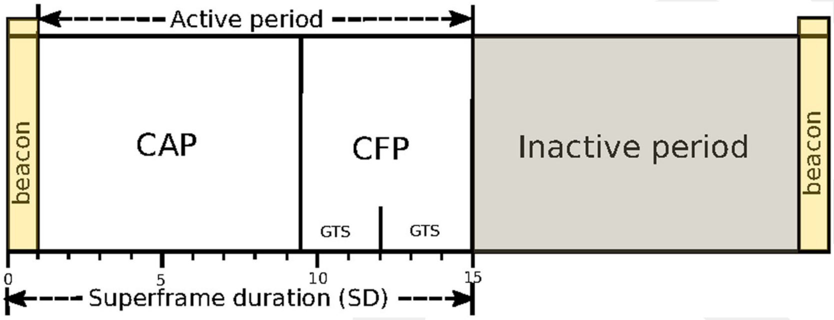


FIGURE 9 Superframe structure of IEEE 802.15.4 beacon enabled mode

FFD at a time. RFDs are used to cater extremely simple tasks like turning on and off an electric switch or sense the temperature. However, it should be noted that the FFD, which serves as the coordinator, does a lot of work compared with the RFD. FFD can carry out full protocol implementations, whereas the RFD can run minimal protocol implementations.

- PHY Layer. The PHY layer operates in unlicensed industrial scientific and medical (ISM) bands. There is a total of 27 channels available across all the bands. Different bands are allocated to different regions as mentioned in Table 4.[96] PHY performs transceiver activation and deactivation, energy detection (ED), link quality indication (LQI) tasks, channel selection, clear channel assessment (CCA), and transmission and reception of the packets across the physical medium. ED and LQI serve as measurement functions, which help indicate the interference level. The CCA capability also provides protection against interference and collisions by allowing the devices to defer transmission in case of channel occupation by another device. CCA is a way to detect any activity on the channel prior to making a transmission attempt. CCA is used as a part of CSMA/CA algorithm and has three modes:
    1. CCA with energy above ED threshold: whenever CCA detects any energy above ED threshold, the medium is reported as busy.
    2. CCA with carrier sense only: CCA reports a busy medium if the detected signal has the modulation and the spreading characteristics of the IEEE 802.15.4, regardless of the signal being lower or higher than ED threshold.
    3. CCA with carrier sense and energy above threshold: the medium is reported busy by CCA upon detecting the signal with the modulation and spreading characteristics of the IEEE 802.15.4 and having energy above ED threshold.
- MAC Layer. The MAC flexibly handles traffic requiring bounded latency or guaranteed bandwidth and the ordinary traffic. Two MAC modes are defined by the standard, *beacon-enabled* (BE) and *nonbeacon-enabled* (NBE), as described next.

- BE mode. In this mode, the PAN coordinator utilizes the superframe structure as shown in Figure 9. The superframe comprises of the active period and inactive period. The active period can be subdivided into 16 equally spaced time slots. The beacon occupies the first slot, and the remaining slots make up the *contention access period (CAP), contention free period (CFP)*, and the inactive period. After the beacon slot, CAP begins, where nodes that have data to transmit, compete using slotted CSMA/CA scheme to gain access to the channel. A typical slotted CSMA/CA procedure is shown in Figure 10. CFP includes a number of contiguous guaranteed time slot (GTS). During CFP, devices use their dedicated GTS to transmit or receive data. GTS mainly handles time-critical or bandwidth reservation traffic of the nodes. In this way, the standard provides a flexible way to handle normal and high priority traffic. A GTS can occupy more than one slot and at most seven GTSs are allowed at a time. The inactive period allows duty cycling where nodes, including the PAN coordinator, can switch-off their transceivers to save energy. The superframe information is broadcast by the PAN coordinator through the beacon frame. This information includes superframe duration, number of GTS allocations, and other network-related information such as synchronization, etc. Every node that receives the beacon joins the PAN through association request and synchronizes with it.
- NBE mode. In this mode, PAN coordinator neither makes use of beacons nor GTS and there is no superframe structure implementation. Rather, the whole active period can act as CAP and implements unslotted CSMA/CA for channel access. The unslotted CSMA/CA procedure is depicted in Figure 10. Devices do not need to synchronize with the PAN coordinator having no synchronization to back off boundaries.[96] Moreover, unslotted CSMA/CA implements a single

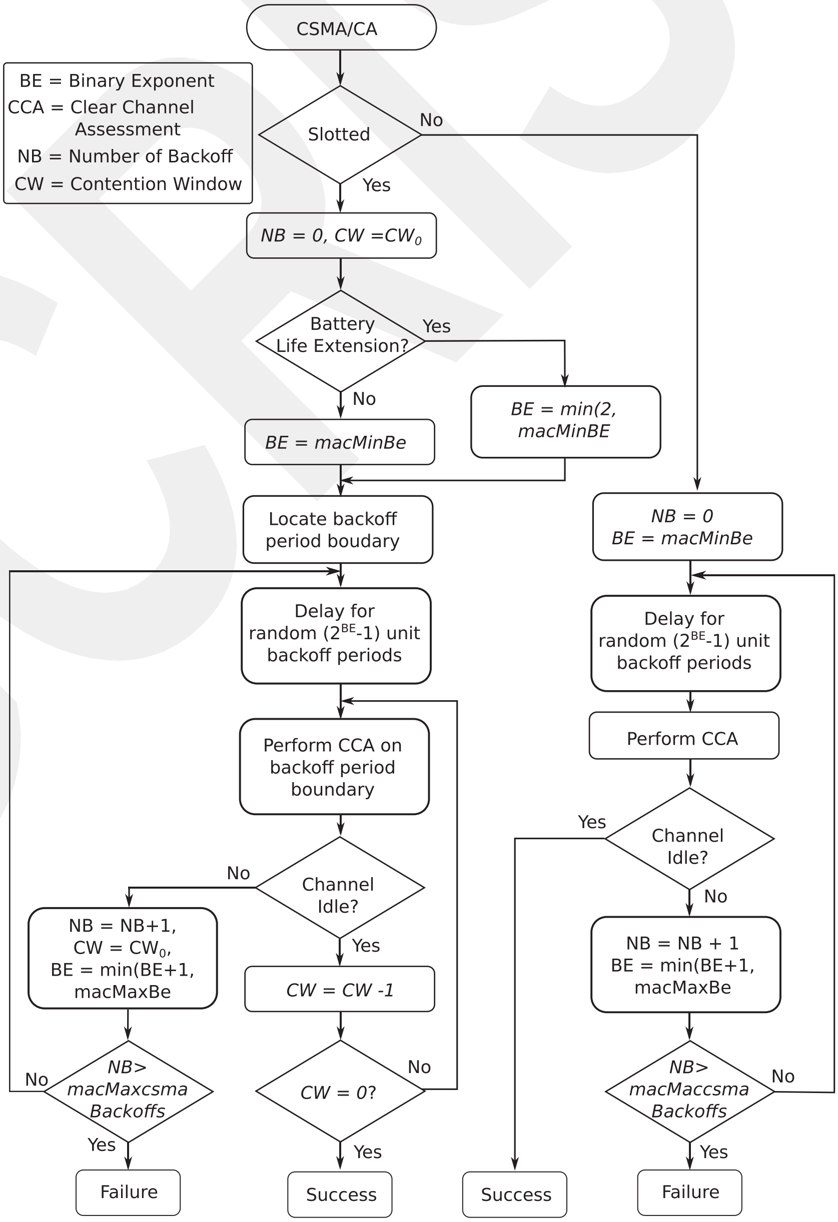


FIGURE 10 Slotted and unslotted carrier-sense multiple access/collision avoidance (CSMA/CA) procedures[96]

CCA operation. The PAN coordinator remains switched on all the time, and every node can follow a different wake-up and sleep schedule. Nodes can only wake up to transmit a data or control packet to the PAN coordinator or receive data through data request and data acknowledgment handshake procedure.[83]

- Limitations of the IEEE 802.15.4 MAC. Although the IEEE 802.15.4 has continued to be the preferred standard across many application domains of WSNs, it severely lacks to support time-critical, energy, and bandwidth-critical industrial applications for medium access. Several limitations of the MAC have been investigated in previous studies.[97-101] For example, Khanafer et al[97] showed that the use of slotted CSMA/CA in beacon-enabled mode results in nondeterministic communication and unpredictable delay for mission-critical applications because of the random distribution of back off period. They provided a comprehensive survey of many MAC protocols, which attempt to solve problems caused by their default MAC design.

Pollin et al[100] analysed the performance of slotted CSMA/CA both with saturated and unsaturated periodic traffic. They showed how the default MAC parameters of the standard such as MAC minimum binary exponent and number of back offs parameters cause energy waste and low throughput. The evaluation of the protocol was done through a Markov model. On the basis of evaluation, the authors suggested to tune the MAC parameters for better energy saving and high throughput.

An investigation on the MAC unreliability problem through extensive simulation and experiments was presented by Anastasi et al.[98] The authors concluded that the behavior of power management mechanism effects energy consumption and results in low *packet delivery ratio* (PDR). The cause was known to be the contention-based MAC and the default values of the parameters associated with it. They suggested more appropriate tuning of MAC parameters for the better reliability in terms of PDR but at the expense of increased energy and delay.

Anastasi et al[102] studied the performance of the MAC in a multihop scenario. They showed that the MAC in its current form has poor performance for energy efficiency, low delivery ratio, and reliability for time-critical industrial applications. They suggested alternative MAC parameters to achieve better results in a multihop scenario. Moreover, the limitations of the GTS scheme in terms of energy efficiency, reliability, and bandwidth utilization were investigated in Koubaa et al, Shrestha et al, and Na et al.[103-105] For example, Koubaa et al[103] argued that GTS is limited to seven which is very small and supports explicit allocation, which results in unfairness and bandwidth waste. They suggested an alternative implicit GTS allocation scheme based on delay and traffic requirements of the communication flows.

Chen et al[106] provided analytical and simulation of the MAC for real-time operation in industrial automation. The authors showed that the GTS-length limits the number of devices to transmit their delay sensitive data and induces delay until all the allocated GTSs are released. Allocation and deallocation of GTSs incur additional delay for real-time operation. Fixed length of CAP adds further constraints on the allocation of GTSs.

Other studies[107-111] analysed BE mode for multihop scenarios, and identified the problem of beacon collisions from different PAN coordinators. This results into loss of synchronization for nodes, thus, they cannot properly follow the superframe structure. Another problem occurs with the overlapping of superframes from two coordinators, which may result in collisions in CFP. Therefore, to avoid these problems, various methods such as beacon scheduling and superframe scheduling are considered. Further studies related to the performance analysis of IEEE 802.15.4 MAC can be found in previous studies.[112-116]

8.1.1 | ZigBee

The ZigBee Alliance[14] is a group of leading companies actively working together to design and develop cost-effective, low-power, reliable wireless networking solutions for WPANs. It is the most widely used standard enabling applications across consumer, commercial, and industrial markets worldwide. It is built on top of the IEEE 802.15.4 PHY and MAC specifications but defines its own network layer. It supports star, tree, and mesh topologies. The standard can be considered as an enhancement to the IEEE 802.15.4, maintaining, supporting, and developing sophisticated protocols for residential and commercial applications. Therefore, these two standards are often confused. ZigBee provides different protocol features from network to application layer. The routing supports mesh networking along with node authentication, encryption, and security. The mesh capability has an added advantage of reliability. Nodes can also serve as intermediate relays to forward and relay traffic to destination forming a multihop network. This makes it suitable for large deployments. ZigBee networks can have three types of devices: ZigBee coordinator, ZigBee router, and ZigBee end devices. ZigBee coordinators are responsible to manage their own network as well as maintain connections with other ZigBee networks. ZigBee routers are like FFDs equipped with additional functionality of routing and maintaining multihop communication. ZigBee end devices can act as RFDs or FFDs, and they only collect and transmit the sensory information towards the router or coordinator.

ZigBee has its own application-level framework for application layer. The application layer defines *application support sublayer* (APS) comprising *ZigBee device objects* (ZDOs) management and manufacturer-defined application objects.[14] The manufacturer-defined objects are used to implement applications which are based on the requirements as suggested by the standard. It supports 240 application objects. Although ZigBee has potential market share especially for home and office applications, the standard has not been adopted by the industrial applications because it cannot provide deterministic delay and high reliability.[117] It shares the same frequency spectrum with IEEE 802.11 and bluetooth, which generate potential interference and cause MAC to frequently back off. This renders the nodes devoid of easy channel access, causing delay for the delivery of time-critical data. ZigBee employs the same MAC as the IEEE 802.15.4, thus it suffers from the same limitations as described in Section 8.1. Therefore, ZigBee has developed its variant called ZigBeePRO[118] to support industrial process and control applications.

8.1.2 | IEEE 802.15.4e

IEEE 802.15.4e[13] is the enhanced extension of the IEEE 802.15.4 standard. It improves upon reliability, deterministic latency, network capacity as well as energy efficiency. The standard does not make any changes in the PHY but only modifies the MAC sublayer. Therefore, it can be used on any IEEE 802.15.4 compliant hardware without any amendment. The standard introduces different methods of channel access in the form of MAC behavior modes namely *time-slotted channel hopping* (TSCH), *Deterministic and Synchronous Multichannel Extension* (DSME), *Low Latency Deterministic Network* (LLDN), *Asynchronous Multichannel Adaptation* (AMCA), and *Radio Frequency Identification Blink* (BLINK). Among these, we focus on TSCH MAC mode because it is considered the most suitable[119,120] for industrial process automation and control applications because of its time diversity and frequency diversity features as explained next.

- TSCH MAC. TSCH employs time-slotted access and channel hopping which offer deterministic channel access and resilience against interference, respectively. The idea of TSCH was first developed by the Dust Network[121] in its propriety MAC called Time-Synchronized Mesh Protocol (TSMP),[122] which was later used by the WirelessHART for its MAC operation. Several industrial standards also adopted TSCH as the core technology and adapted the upper layers and frame formats to meet their specific needs. TSCH follows the *slotframe* structure as shown in Figure 11, which shows time divided into fixed length slots known as *time slots* and depicts a typical sequence of events taking place between a sender and receiver pair for an acknowledged communication. With the use of channel hopping, each transmission occurs on a different channel; for instance, in case of IEEE 802.15.4, 16, channels are available to hop through. A slotframe groups a number of time slots. A time slot is long enough to handle a transmission of maximum length packet and receive an ACK from the receiver. Slotframes are repeated over time to enable participating nodes to have periodic access to the channel. Each node in the network follows a schedule which tells the nodes when to transmit, receive, or sleep. During the sleep period, nodes can turn off their transceivers to conserve energy.

  A TSCH link is essentially represented by a time slot (TS) and a channel offset (CO), ie, Link = (TS, CO). A frequency for a given link can be computed through Equation (1).

$$frequency = F[(CO + ASN)\, mod\, nFreq], \tag{1}$$

  where *absolute slot number* (ASN) acts as a time slot counter shared by all the devices. ASN is initialized to 0 at the start of the network and is incremented globally in the network at every time slot.[13] F contains the set of available channels, $nFreq$ is the size of F. Channel offsets can be as many as there are available frequencies, even if the two nodes have the same channel offset, but a different ASN will translate into a different frequency. Figure 11 shows a slotframe which contains eight time slots and 16 channel offsets. A slot represents a TSCH schedule, which is similar to a matrix of width equal to the slotframe size and of height equal to the number of available channels. Nodes only care for the cells in which they participate. For example in Figure 11, when node n_9 has a packet to send to node n_6, it waits for slot numbered 4, and sends it on channel offset 15. It can stay off for the other cells. If n_6 has packet to send to n_7, then it uses slot numbered 6 and channel offset 0. Moreover, there are two kinds of slots, *shared slot* and *dedicated slot* as depicted in Figure 11, for example, the nodes n_1 and n_3 use a shared slot in which both nodes try to transmit at the same slot offset and channel offset. Collision can occur in shared slots, which is resolved by a simple back off mechanism as defined by the standard. Besides, synchronization is the crucial requirement to maintain the connectivity with the neighbor nodes. Therefore, TSCH uses *acknowledgement-based synchronization* and *frame-based synchronization* methods. Acknowledgement-based synchronization involves receiver calculating the delta between the expected time of frame arrival and its actual arrival time, and providing this information to the sender in the

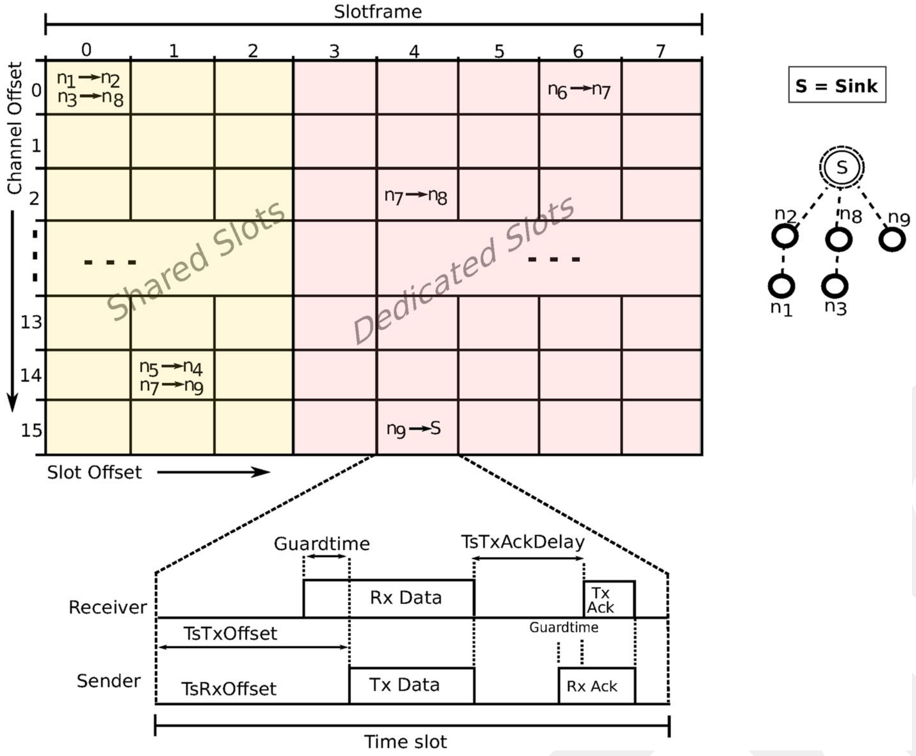


FIGURE 11 A, Time-slotted channel hopping (TSCH) slotframe showing dedicated and shared slots for the associated topology in B, It also depicts typical sequence of events taking place within a slot between a sender and a receiver

acknowledgment. This way, the sender adjusts its clock based on the receiver's clock. In frame-based synchronization, the receiver synchronizes with the clock of the sender by calculating the delta between the expected time of a frame arrival and its actual arrival time and adjusting its clock by the difference.

Although TSCH MAC design goals are technically promising, more studies need to be conducted to test the practical performance of the MAC before using it in commercial deployments across the industrial domain. Some recent studies have been conducted,[119,123-125] but they only focus on analytical models and simulations. They do not provide realistic performance in experimental set-ups. Only very few test bed studies have been conducted, which can be found in Vilgelm et al and Yaala and Bouallegue.[126,127] More experimental studies are required to test the performance of the MAC to be successfully deployed in IWSAN applications.

- TSCH MAC deficiencies. One important feature that is missing in TSCH is the provision of communication schedule. There is no mechanism that can help to build and maintain the communication schedule. Although TSCH defines how to execute centralized, distributed, or hybrid schedule, building and maintaining an optimal and reliable communication schedule is still an open research problem.[128] Several studies related to link scheduling have been carried out, which can be found in previous studies.[129-134] Further, TSCH network formation involves transmission of *enhanced beacons* (EBs). EBs work similar to beacons like in IEEE 802.15.4 network and help maintain synchronization, topology, and other network parameters but the standard does not mention and specify mechanism related to the EB advertisement and configuration.[135] To overcome this issue, a model-based optimal beacon scheduling algorithm has been proposed in De Guglielmo et al.[136]

  Other works[137,138] studied the performance of TSCH protocol in co-located environments, where multiple instances of the protocol were run in different neighboring networks taking clock drifts into account. Authors revealed that the protocol faces periodic interference that results collision from other nearby networks, which deteriorates its performance for reliability. They showed that as the density of the network increases or the number of networks grows, the collisions occur more frequently.

  Further, the recent efforts are to integrate IPv6 with TSCH as explained next.
- IPv6 over TSCH. Standardization efforts in the 6TiSCH (IPv6 over the TSCH mode of IEEE 802.15.4e)[139] workgroup at Internet Engineering Task Force (IETF)[140] aim to integrate IPv6 into TSCH to foster convergence between low-power wireless networks and the *Internet Protocol* (IP). The workgroup defines a new sublayer 6top (6TiSCH Operation Sublayer),[141] which provides support for central, distributed, and hybrid scheduling. 6top makes a network connectivity

graph and accordingly allocates resources to the nodes. It issues commands to upper layers to set specific schedules based on the latency and bandwidth requirements.[141]

8.2 | Industrial standards

Several industrial standards have been developed over the last decades, such as WirelessHART,[19] ISA100.11a,[20] and Wireless Networks for Industrial Automation-Process Automation (WIA-PA).[21] These standards employ two major existing wireless technologies; IEEE 802.11[13] and IEEE 802.15.[142] The former is widely recognized as Wireless Local Area Network (WLAN) and the latter as Wireless Personal Area Network (WPAN). Both technologies target different application scenarios with their corresponding merits and demerits.[142] Initially, these technologies were not conceived to be targeting industrial automation. Generally, IEEE 802.11 was designed to offer high data rate up to tens of Mbps, requiring transceivers to operate with large energy consumption, whereas, IEEE 802.15 offering low data rate from Kbps to several Mbps and requiring low energy transceivers. Because of high energy budget of WLANs, their application to IWSNs is not suitable as sensor nodes are energy constrained and cannot withstand such a large energy budget.[84] Therefore, standards targeted IEEE 802.15 based solutions.

The IEEE 802.15 is further divided into two groups; IEEE 802.15.1 and IEEE 802.15.4. The IEEE 802.15.1 is known as bluetooth, it falls between IEEE 802.11 and IEEE 802.15.4 with respect to data rates and energy consumption. Although bluetooth supports higher data rates compared with IEEE 802.15.4, its energy consumption is higher and is, therefore, less suitable for low-power requirements of wireless sensor nodes. One of the protocols based on IEEE 802.15.1 is Wireless Interface for Sensor and Actuators (WISA),[143] developed by ABB targeting strict real-time requirements of communication among sensors and actuators and is considered an IEEE 802.15.1 based standard solution. In comparison with IEEE 802.15.1, the IEEE 802.15.4 is designed targeting WSNs and meeting their low energy requirements, offering moderate to low data rates. Therefore, it is widely used standard for WSNs in general and IWSNs in particular. Several industrial standards like ZigBee, WirelessHART, ISA100.11a, and WIA-PA use IEEE 802.15.4 as the core technology to support different applications in industrial process automation.

In the following discussion, we give an overview of two well-known industrial standards based on the IEEE 802.15.4 standard.

8.2.1 | WirelessHART

WirelessHART[19] is the first attempt to provide a complete standard solution for industrial process control applications. A basic network architecture of WirelessHART is shown in Figure 12. The major motives behind the development of WirelessHART were precisely to offer viable solutions to meet strict timing and heavy interference issues in the industrial environment. It is a complete protocol suite developed by the HART foundation and is backward compatible with the HART legacy systems, it is self-organizing and self-healing. As compared with wired HART, most of the modifications in WirelessHART have been made in PHY, MAC, and network layers. WirelessHART network consists of eight different types of devices such as network manager, security manager, gateway, access points, and field devices, adapter, router, and hand-held devices. All devices except field devices are employed to support network-related activities like network formation, configuration, maintenance, routing, reliability, and security. The field devices (sensors, actuators) are directly connected to the plant equipment or processes and can be organized in star or mesh topologies. Mesh topology provides additional reliability by providing redundant paths.

- WirelessHART MAC. On top of the IEEE 802.15.4 PHY, WirelessHART uses its own MAC protocol, which uses a TDMA-based superframe structure along with frequency diversity and is known as TSMP.[122] The MAC uses the same principle as TSCH as mentioned in Section 8.1.2. The time slot has a fixed duration of 10 ms to transmit a maximum size packet (133 Bytes including header) and receive an acknowledgement. A single slot can utilize 15 channels, so in theory, a total of 15 devices can transmit/receive packets simultaneously.

  Numerous enhancements like security and reliability have also been embedded. It also includes built-in time synchronization. The standard introduces a network manager, which takes care of a lot of heavy computational tasks and employs several significant attributes like communication schedule assignment and maintenance, routing management supporting redundant routing paths to increase reliability. This way, the network manager has the global view of the network, which makes it easier to efficiently look after transmission and security of the overall network. A dedicated security manager exists which collaborates with a network manager in order to protect the network from intrusions and attacks by generating session keys and network keys for all the devices. Thus, provides end to end data integrity[144] at MAC and network layer. To cope with the unreliability issues of a wireless channel, the standard utilizes channel

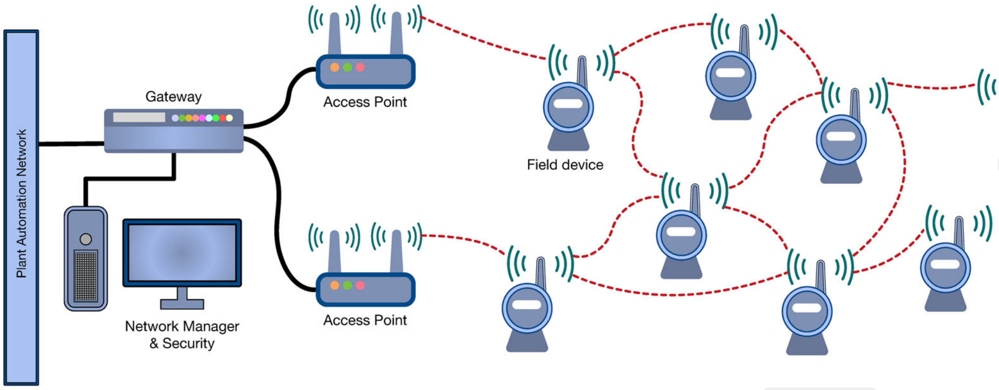


FIGURE 12 WirelessHART network architecture[19]

hopping and channel blacklisting to mitigate multi-path fading and interferences. Blacklisting is the way to disable certain channels that have poor performance; the channels which are blacklisted cannot be used in channel hopping, in this way, nodes do not use those channels. Although these features are the most preferred standards, it is still emerging and requires improvements. For instance, the nodes cannot directly connect to the Internet without gateway.[145] The standard lacks improved scalability because of TDMA-based MAC protocol, which limits the number of nodes participating in the network due to latency, synchronization, and other QoS requirements.[31] The standard supports centralized architecture, which also imposes further constraints on the scalability. Further, the standard operates in ISM band which is already crowded, making it more vulnerable to interference.

8.2.2 | ISA100.11a

The standard has been developed by ISA[20] to offer secure and robust communication for industrial process automation and control applications. The PHY layer of the standard is IEEE 802.15.4-compliant and employs frequency hopping and channel blacklisting to improve robustness against interference from other coexisting networks.[20]

The MAC sublayer utilizes a combination of contention-based and schedule-based approaches. The network layer supports IPv6 over Low Power WPAN (6LoWPAN)[17] protocol to enable it to be connected to the Internet. The transport layer supports flow control, segmentation, reassembly, and also security. It has the ability to support both end-to-end acknowledged and unacknowledged communications.[146] Mesh and star topologies or combinations of both are supported by the standard. The ISA100.11a network comprises of sensors and actuators known as input/output (I/O) devices, which are basic field devices for sensing and actuating tasks. Routing devices ensure selection of routes towards the destination in mesh networks in multihop fashion and in case of primary routes failure, alternatives routes can be selected to guarantee reliability. The backbone routing device is responsible to connect to external networks by performing ISA100.11a-compliant packet encapsulation. The gateway device serves as an interface between the plant network and ISA100.11a field network. The system manager performs network run time configurations, monitors communication configurations, including slot allocation and scheduling. Finally, the security manager executes policies of security standards. [148]

- ISA100.11a MAC. The MAC takes a hybrid approach combining TDMA and CSMA/CA, together with additional spatial, frequency, and time diversity to achieve real-time performance. However, in case of strict delay requirements, CSMA/CA can be disabled.[146] TDMA exploits frequency hopping to enable multiple devices to transmit simultaneously on different channels provided that only a single device may communicate on one channel per time slot.[149] TDMA supports configurable time slots, which means the duration of slot and superframe can be changed flexibly by modifying the two MAC parameters; *TsDur* and *SfPeriod*. Typical time slot duration ranges from 10 to 12 ms.[147] Time slot configuration employs *slotted hopping*, *slow hopping*, or *hybrid hopping* as shown in Figure 13. Slotted hopping enables nodes to transmit at prescheduled TDMA slots and the channel offset, thereby avoiding interfering channels.[60] While in slow hopping, a single channel employs a collection of successive time slots in a period between 100 to 400 ms as configured by the system manager.[147] Slow hopping does not use TDMA but uses nondeterministic CSMA/CA to provide immediate channel bandwidth on demand, which supports event-based traffic in which certain events may cause the need for a device to immediately transmit an alarm or data packet. While in slotted hopping, a device is forced to wait—it is only allowed to transmit in the next scheduled slot—which causes latency to increase for event-based data

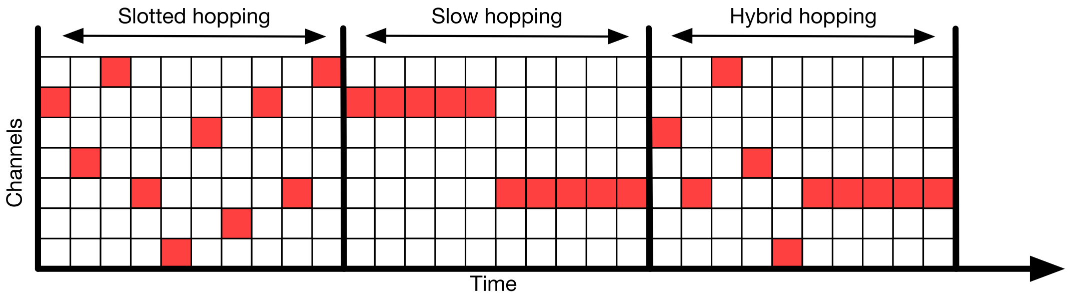


FIGURE 13 Medium access control (MAC) with slotted and slow hopping in ISA100.11a[60,147]

transmissions. [149] Slow hopping results in more power consumption than slotted hopping since it renders the receivers to continuously listen to the channel for incoming traffic.[147] Finally, the hybrid hopping combines both the slow hopping and the slotted hopping and flexibly switches between the two.

8.2.3 | Wireless Networks for Industrial Automation-Process Automation (WIA-PA)

WIA-PA[21] was introduced by the Chinese Industrial Wireless Alliance (CIWA)[150] in 2008 and is the national standard of China. It is another approved standard by the International Electrotechnical Commission (IEC) as IEC-[151] in 2011 after the WirelessHART. The standard offers communication specifications and architecture for the process automation applications. It is based on the IEEE 802.15.4 standard and implements an improved version of the MAC by using three frequency hopping schemes, which enable it to intelligently cope with the varying network conditions. The MAC takes a mixed approach by utilizing hybrid approach that uses contention-based and reservation-based mechanisms. WIA-PA network uses five types of physical devices: host computer (user interface for management and maintenance), a gateway device (connects other networks in the plant), routing device (forwards packets through multiple device in multihop networks), field device (controls or monitors handheld devices), and handheld device (sensors and actuators to monitor and control the production plant).[152] It supports combination of star and mesh network architectures in an hierarchical way, ie, the routers communicate through mesh topology while the handheld devices, field devices, and routers communicate using star topology. WIA-PA recommends reactive approach to enhance further reliability and self-healing by using redundant routing and gateway devices to avoid network failures.[153] To conserve energy, WIA-PA uses two-level packet aggregation schemes natively: data aggregation at the application layer and packet aggregation at the network layer, whereas WirelessHART and ISA100.11a utilize one-level packet aggregation. It also employs security manager and network manager. The former implements and manages security keys and authentication, whereas the later configures the network, schedules communication, handles routing table, and looks after the overall network.

- WIA-PA PHY and MAC Layer. The PHY is IEEE 802.15.4-2006-compliant, same as the WirelessHART and ISA100.11a. The MAC is built on the BE mode superframe structure and uses CSMA, TDMA, and FDMA approaches. Unlike the IEEE 802.15.4 standard MAC, the WIA-PA MAC implements node joining, intercluster management, and retransmissions during the CAP of the superframe.[154] Although the inactive period of the superframe is used for duty cycling to save power of the nodes, however, a part of it is also used for the intracluster and intercluster communications. It supports *adaptive frequency switch*, *adaptive frequency hopping*, and *time slot hopping*,[152] which make it highly reliable, self-organizing, and self-healing, thus, it can reliably coexist with other networks. The MAC can define frame priorities and there are four kinds of priorities—highest, secondary, third, and lower priority—and the schedules can be allocated on the basis of the priorities. The synchronization at the MAC is maintained through a time source, nodes take gateways as time source in intercluster communication and routers in intracluster communication.

  Further, there are increasing demands to enable IPv6 datagram to be transported over WIA-PA network, one such scheme is proposed and evaluated in Wang et al.[153]

8.2.4 | Comparison of industrial standards

Table 5 presents different wireless standards along with their PHY and MAC layer features. The comparison takes into account different performance metrics that each standard tries to satisfy.

TABLE 5 Comparison of low-power wireless standards

Feature	WirelessHART	ZigBee	ISA100.11a	WIA-PA	IEEE 802.15.4e
Physical and MAC Layer					
PHY Layer	IEEE 802.15.4-2006	IEEE 802.15.4-2003	IEEE 802.15.4-2006	IEEE 802.15.4-2006	IEEE 802.15.4
Data rate	250 kbps	250 kbps	250 kbps	250 kbps	250 kbps
MAC scheme	TSMP (TDMA, CSMA)	GTS, CSMA	TDMA, CSMA	TDMA, CSMA	TSCH (TDMA, CSMA)
Slot duration	Fixed (10 ms)	Flexible	Configurable	Configurable	Flexible
Frequency hopping	Yes (blind)	No (frequency agility)	Yes (blind)	Yes (adaptive)	Yes (blind)
Network topology	Star, Mesh	Tree, Star, Mesh	Star, Mesh	Star, Mesh	Star, Mesh
Implementation	Simple	Simple	Complex	Medium	Simple
Frame-based priority	Yes	No	Yes	Yes	No
Channel blacklisting	yes	No	Yes	No	No
Metric comparison					
Reliability	✓	✗	✓	✓	✓
Deterministic latency	✓	✗	✓	✓	✓
Scalability	✗	✓	✓	✓	✓
Energy efficiency	✓	✓	✗	✗	✓

Abbreviations: CSMA, carrier-sense multiple access; GTS, guaranteed time slot; MAC, medium access control; TDMA, time division multiple access; TSCH, time-slotted channel hopping; TSMP, Time-Synchronized Mesh Protocol.

9 | MAC PROTOCOLS FOR CRITICAL DATA DELIVERY IN IWSAN

Apart from industrial standards, we have witnessed other non-standard MAC protocols that can be used in IWSAN applications because they target to support their critical requirements. Some of these representative protocols can be used as part of the wireless standards such as WirelessHART and ISA100.11a. Since wireless standards are more of a framework than complete solutions, these protocols can be helpful for many of the industrial scenarios. We provide a brief description of these protocols focusing on how their MAC design impacts different performance metrics, we also highlight their advantages and disadvantages.

9.1 | GinMAC

Suriyachai et al proposed GinMAC,[82] a TDMA-based MAC protocol for the largest European project named GINSENG.[62] The deployment of the project was carried out in the largest oil refinery plant located at Sines, Portugal. GINSENG offers a solution to implement performance control for closed-loop control applications using WSN. The protocol is designed to support reliable and timely data delivery in industrial process automation. It aims to meet requirements of bounded delay from the sensor to the sink as well as from sink to actuators. It is based on the tree topology and comprises of the following unique attributes like *off-line dimensioning process*, *exclusive TDMA*, and *delay conform reliability control*.

In off-line dimensioning, the application traffic patterns and channel characteristics are determined before deployment. Calculations of transmission schedule are performed off-line and predeployment. Therefore, the protocol exhibits predictable performance. TDMA frame consists of basic slots, additional slots, and unused slots. Basic slots are used by sensors such that within the frame length F, each sensor forwards one message to the sink and the sink can forward one message to each actuator. Additional slots are used exclusively for reliability purpose in order to improve reliability control. Finally, unused slots are used purposely to introduce duty cycling to conserve energy of the nodes. In exclusive TDMA and delay conform reliability control, fixed size TDMA slots are used. An exclusive slot is only used by its owner and cannot be reused by other nodes.

Although GinMAC suitably tailors to control loop applications where the data must reach the sink in a converge-cast pattern, which is common in IWSAN scenarios, it has some limitations for scalability. The protocol does not support large number of nodes. It is restricted to only 25 nodes because of exclusive TDMA slot usage. This restriction is not a problem for the targeted application. However, to make this protocol more usable in IWSAN scenarios that require a large number of nodes, it needs much improvement for scalability.

9.2 | PriorityMAC

Shen et al[155] proposed PriorityMAC protocol for critical traffic in IWSAN. It is a priority-enhanced MAC protocol and provides service differentiation for traffic categories of different priorities. The priority mechanism enables high priority traffic to hijack the transmission bandwidth of low priority traffic.[155] It considers three kinds of traffic categories according to priority like safety, control, and monitoring. Among them, safety is the most critical, then control, and finally monitoring. The traffic needs to be transmitted with low latency and high reliability according to its priority. The critical traffic is prioritized over noncritical traffic in order to avoid system instability and losses, because the unpredictability regarding the arrival of critical traffic (aperiodic traffic) creates difficulties with regard to making a suitable scheduling or reserving the wireless bandwidth. It employs WirelssHART and ISA100.11a as a baseline, and offers a MAC mechanism to improve access for critical traffic. The experimental evaluation shows a reduction of 94% latency for high priority traffic and 93% for secondary priority traffic on average. The experiment was conducted through TinyOS on TelsoB motes. The working principle of the protocol is that it employs four distinct access methods (AM) concurrently operating within the protocol and meeting requirements of different traffic categories (TC). Each of the TC conforms to one AM. There are four traffic categories denoted as TC1, TC2, TC3, and TC4. Each of them uses its corresponding AM for medium access. TC1 has the highest priority over TC2 and then TC3 and TC4. TC3 and TC4 utilize TDMA, and TC2 uses joint back off and indication approach. When there is a TC2 packet that has to be transmitted, it starts a back off process. During back off, it sends a jamming indication to defer the attempts of TC3 and TC4, meanwhile it also takes care of the same or the high priority traffic by listening to the medium so that any possible collisions can be avoided. TC1, having the highest priority, persistently sends jamming indication until the channel is found idle, after that, it begins transmission. The design strategy is that the PriorityMAC can hijack time slots of low priority traffic by deferring and even destroying its attempt and transmission. There is a set of access methods for PriorityMAC and high priority indication space (HPIS) associated with AM to differentiate the channel access. TDMA access mechanism within the protocol works by an algorithm, which utilizes time slot series known as superframe duration to allocate bandwidth to each communication link. Thereby, allowing each link to get a periodic chance to utilize its dedicated slots to transmit its packets. A slot is then further divided into a series of subslots considered as minimum time unit. HPIS is introduced and is composed of two subslots. HPIS is inserted between the end of a slot and the start of the next slot. It allows high-priority traffic while deferring the lower priority traffic, alongside, it also avoids collisions with same or high priority traffic. Although the protocol provides packet differentiation, the design complexity is very high. Moreover, the access delay of high priority traffic is nondeterministic.

9.3 | QoS-MAC

Suriyachai et al[156] proposed a QoS-aware MAC protocol, which aims to provide predictable end-to-end message transfer delay and reliability. Authors define a collision-free TDMA schedule by employing fixed length time portion known as epochs. A node having no data to transmit in its reserved epoch simply transmits a control signal to its parent indicating no transmission. Cross-layer approach is employed by embedding routing at MAC. Topology awareness is built in the MAC layer to ensure deterministic end-to-end transport performance. Each node follows a different duty cycle to save energy depending on its position in a predetermined tree topology. Retransmission slots are reserved to cope with the wireless errors and consume extra energy. Although the design aspects of the protocol match the IWSN application classes that require different QoS guarantees, synchronization problems can occur frequently due to clock drifts in child-parent sensor nodes. Proper slot assignment and duty cycling require each nodes to determine their position in the tree which causes the protocol not to scale well for large networks.

9.4 | WirArb

Wireless arbitration (WirArb) is priority enhanced MAC protocol[157] targeting IWSAN applications. It is based on different arbitration frequency levels, which gives an ordered channel access to each network device. In this way, nodes with highest priority gain immediate access to the medium and thus achieve real time performance for time-critical traffic. Zheng et al consider TDMA to be less suitable for safety systems in industries because these systems need immediate response to trigger and cannot wait for their dedicated TDMA slots to proceed with their transmission.

The arbitration phase of the protocol consists of two phases: *arbitration decision* period, which processes the channel access requests and determines a channel access order, while *arbitration execution* period handles the data transmission. In this way, a node having the highest priority accesses the channel first. The network nodes need to forward their channel access requests to the gateway prior to data transmission. This requires all the devices to be synchronized with the gateway. For the gateway to identify different channel access request signals, a new PHY mechanism has to be built in both the receiver's gateway and the transmitter of the network devices. In this way, the event priorities are mapped with sub-carrier frequencies. Each device is pre-assigned a specific subcarrier frequency and these frequencies remain orthogonal to each other.

Although WirArb promises to meet hard real-time requirements with predictable performance, it adds complexity into the existing PHY layer. Besides, the protocol does not explain how the devices send their channel access requests to the gateway and synchronize with the it. With increasing number of devices, the channel access requests increase and can cause access competitions. Moreover, the protocol is only evaluated analytically through discrete Markov chain, therefore its practical performance remains to be determined. The protocol is still in its early stages of development and several challenges need to be resolved for its actual deployment.

9.5 | Breath

Park et al[75] suggested Breath, an adaptive protocol for industrial control applications for reliable and timely data transmission while minimizing energy consumption. The protocol is a simple cross layer protocol based on randomized routing, CSMA/CA MAC, and duty cycling. The basic design scheme depends on a constrained optimization problem where the objective function is the energy consumption and the constraints are the reliability and delay. The authors give a clear analytical relation among reliability, delay, and energy consumption as a function of MAC, routing, and duty cycle. They systemically verify their approach based on sound approximations. An adaptive algorithm is proposed which dynamically adapts to the network traffic and channel conditions as per the application requirements. A feedback based control loop scenario is considered consisting of plant, sensors, and controller. The goal is to remotely control the plant over a multihop WSN. Multihop capability is achieved through cluster based topology with *h-1* relay clusters. A data packet reaches the sink through relay clusters taking a multihop route. Breath uses randomized routing instead of fixed routing approaches

TABLE 6 Comparison of MAC protocols based on different performance metrics

Protocol Metrics Comparison				
Protocol	**Reliability**	**Delay**	**Energy efficiency**	**Scalability**
Priority MAC	✗	✓	✓	✗
QoS MACS	✓	✓	✓	✗
WirArb	✓	✓	✗	✓
Breath	✗	✓	✓	✓
GinMAC	✓	✓	✓	✗
DMA-MAC	✓	✓	✗	✗

because it offers flexibility for mobile equipments and reconfiguration for control applications. On the other hand, fixed routing schemes impose considerable overhead of maintaining routing tables.

Evaluation of the protocol was done on a testbed with TinyOS and Tmote sensors in indoor environment with AWGN and Rayleigh fading channels. The protocol outperformed an IEEE 802.15.4 implementation with respect to energy efficiency and reliability. Though, Breath targets control and actuation applications but with the use of CSMA scheme while adapting to varying network conditions, the protocol cannot offer high reliability for these applications which characterize precise process models.

9.6 | Dual-mode adaptive MAC (DMA-MAC)

Kumar et al[158] proposed DMA-MAC protocol which is specifically designed to support feedback based process control applications for IWSAN. It is based on TDMA superframe structure and mainly focuses on two operational states of feedback-based process control namely: *transient state* and *steady state*. The protocol meets varying traffic requirements of both operational states of the control hence dual-mode (having two modes). The design of the protocol is mainly influenced by the GinMAC protocol with some changes to support two operational modes. It aims to support key performance metrics such as reliability, predictability, throughput, low delay, and energy efficiency. The protocol switches between two operating modes and the act of switching is a critical procedure. Switching takes place based on a predefined threshold breach observed by the sensor nodes. The transient to steady state mode switch is performed on the basis of preset characteristics, whereas the steady to transient state switch is observed and notified by the sensor nodes to the sink. Because of its dual-mode ability, it handles large traffic loads of transient state and switches back to the steady state adaptively to support low traffic loads and conserves energy. It has two separate superframes, one for the transient state and the other for the steady state. The protocol considers the network manager as an integral part of the overall network solution and can be used as a part of the wireless standards like WirelessHART and ISA100.11a. The superframe has notification slots for state switch notifications, sensors slots to transmit the sensor measurements to the sink, retransmission slots to enhance the reliability, controller slot to process control decision, actuators slots to receive commands from the controller via the sink, alert slots to alert the sink to switch for the operational modes, and sleep slots to conserve energy. Although the protocol takes into account the process dynamics and service differentiation, it has some limitations for scalability. It is limited to only 25 nodes and does not scale well because of TDMA usage and strict delay requirements. Because of the dual-mode nature, the protocol has a complex protocol design resulting in a large code space, which affects the hardware.

9.7 | Comparison of MAC protocols

Table 6 gives the comparison of the all the aforementioned protocols. This comparison is based on different performance metrics that each protocol targets to improve. Although all these MAC protocols try to satisfy the stringent requirements of IWSAN applications, they do not fully conform to all the performance metrics. Therefore, more research is needed in developing MAC schemes. The goal is to overcome the existing challenges and focus on future research directions while proposing new protocols that can help realize the smart industry initiatives. Therefore, our next discussion revolves around existing challenges and future directions.

10 | IWSAN CHALLENGES AND FUTURE DIRECTIONS

IIoT[159,160] is the major breakthrough which promises to revolutionize the industries and lead to the Industry 4.0 revolution.[10,161] The advancement in IWSAN is the foundation to strengthen Industry 4.0. Several standards, protocols, and techniques have been proposed to advance the concept of IWSAN, however, their practical implementations posed several limitations and challenges, which need serious practical solutions. Therefore, future research on protocol design has to focus on these challenges and look for appropriate design alternatives to avoid similar limitations and weaknesses in the future. Below, we highlight important future directions that should be taken into account when proposing new protocols.

10.1 | Scalability

Scalability refers to the ability of a system to scale well or provide a high degree of flexibility.[76] It supports adaptivity to changes with respect to addition and removal of nodes or functionality without degrading its existing performance. Generally, IWSAN may require hundreds or even thousands of nodes, therefore, communication protocols need to be scalable to comply with such requirements. However, the development of scalable MAC protocols is a nontrivial task and imposes a huge challenge. Existing wireless standards such as WirtelessHART and ISA100.11a largely utilize TDMA-based protocols, which impose strict constraint on the number of participating nodes and at the same time satisfy application QoS requirements. Besides, they both follow centralized approach which cannot easily adapt to abrupt changes as required by industrial applications.[60] Therefore, in order to achieve better performance, IWSANs require protocols that can support scalability at different layers of the protocol stack.

10.2 | Promote coexistence

IWSANs require low-power wireless networks to constructively coexist with one another and with other technologies and standards. It is envisaged that the number of connected devices will grow exponentially in the near future, which may cause massive interference. Most of wireless standards operate in ISM band, which has left the band more crowded causing cross technology interference and self-interference.[162] Although current wireless standards exploit channel diversity and time diversity techniques as in WirelessHART,[163] ISA100.11a, and IEEE 802.15.4e to negate the effects of interference so as to promote coexistence, industrial environment introduce potential sources of interference such as electric motors, inverters, ignitions systems, voltage regulators, generators, frequency converters, thermal noise, friction-induced noise, and other RF signals.[73] Because of these, deep fades and channel impairments cause packet loss and link failures. Therefore, PHY and MAC layer schemes need to be well exploited to intelligently avoid such adverse effects and make the network more resilient.

10.3 | Distributed architecture and mobility

Distributed architectures and protocols can conveniently support scalability and manage dense networks and failure of a single device does not lead to overall network failure.[164] Every network device shares the load of computation and processing. Further, distributed network architectures can flexibly cope with the dynamic environment such as networked mobile robots working in dangerous areas or nuclear power plants. High mobility and varying network topologies are adequately supported by the distributed approach, whereas centralized approaches cannot cope with the dynamic scenarios and mobile nodes. Besides, centralized approaches become a bottleneck when the network is scaled up.[60] In multihop networks, distributed architectures are more suitable compared with centralized approaches. However, these architectures come at the cost of increased complexity and large overhead for maintaining and managing the overall network. [131]

10.4 | Interoperability across protocols and standards

IWSANs require new standards and solutions be compatible with existing infrastructure in order to collaboratively support one another. The need to upgrade the existing infrastructure with addition of new functionality requires that the new standards can coexist reliably. Therefore, interoperability supports the seamless integration of new solutions and functionalities into existing processes and systems.[165] Further, IWSAN is a heterogeneous environment having wired networks, legacy systems, and other wireless solutions working together, which cause heterogeneity across protocols, interfaces, and subsystems.[166] The standards like wirelessHART, ISA100.11a, and WIA-PA have many features in common but lack compatibility with each other, so convergence is by getting all these standards to adopt same protocols in order to promote interoperability. Therefore, new protocols and standards should encourage open solutions and uniform frameworks to enhance interoperability.

10.5 | Joint support for sensors and actuators

IWSANs include several processes distributed over multiple locations, which cause each actuator node to serve as a sink for a group of sensor nodes. Managing and coordinating multiple sinks and communication among them increase the complexity of the network management.[1] Most of the existing MAC protocols mostly focus on the sensor-to-sensor or sensor-to-central coordinator (sink) communication only. They are not designed to work well with sensors-to-actuators and actuators-to-actuators communication.[2] As discussed in Section 5.1, actuators are different from sensors since actuators precisely make appropriate adjustments on the basis of the controller decision. Therefore, they impose strict constraints on latency and reliability.[8] This requires that new standards and protocols targeting IWSAN should equally be optimized for sensors as well as for actuators.

10.6 | Cross-layer design schemes

Most of the communication solutions tailored to WSNs are based on the layered protocol architecture of the OSI model because of its to simplicity and modularity.[84] However, because of the constrained resources of WSNs, the increasing trend is to utilize the cross-layer approach in developing protocols in which two or more layer can coordinate and share the information with each other to optimize network performance. Significant energy improvements have been achieved through cross-layer design for the WSN in previous studies.[167-169] The interlayer interactions utilize layer-specific properties to work as a unified framework to reach better results. For instance, the interference and multi-path effects at the PHY layer effect the MAC layer, similarly schedules construction at the MAC layer is influenced by the decisions taken by the routing layer. The trade-off complexity at the MAC layer among various performance metrics cause degradation for many QoS parameters and this can can be greatly balanced through cross-layer interactions. IWSANs protocols need to follow a cross-layer interaction to achieve required balance among reliability, low latency, scalability, and energy efficiency. However, cross-layer protocols come at the cost of increased complexity, hence, versatile schemes are required to reduce this complexity.

10.7 | Security

Security of wireless networks is more challenging as compared with wired networks, because wired networks can physically restrict the network to a desired premise through wires.

Whereas, the wireless network cannot be restricted to desired geographic locations because of signal propagation, which makes it vulnerable to security attacks. WSNs are not an exception to the security, they are susceptible to various security attacks such as denial of service, node tampering, node control, network injection, interference,[170] etc. Protection against these risks should guarantee a secure communication especially in the context of IWSAN. Hence, security should be taken as an integral part IWSAN solutions. The security measures in protocols should take into account the objectives of confidentiality, integrity, authentication, and nonrepudiation during the entire communication flow.

The major industrial standards take security as an integral part of the communication by providing a dedicated security manager such as in WirelessHART, ISA100.11a, and WIA-PA.[171] WirelessHART provides security features both at the MAC and network layers, it uses encryption mechanisms at the MAC, while the network layer ensures data integrity. ISA100.11a provides security both at the MAC and transport layers. MAC offers hop-to-hop security, whereas transport layer handles end-to-end security. Besides, it generates symmetric keys for both message integrity and confidentiality and optional asymmetric keys for the devices that wish to join. Though, security is crucially important, yet it incurs additional overhead and puts lot of processing and computational burden on constrained sensor nodes, which consume energy. Therefore, a balanced trade-off between security schemes and energy consumption should be ensured so that limited resources are not wasted. Further studies on security issues can be found in Walters et al, Wang et al, and Chen et al. [172-174]

11 | CONCLUSION

IWSANs are the gateway to the IIoT, which serve as a ubiquitous infrastructure for the Industry 4.0. This imposes requirements of high reliability, low latency, scalability, energy efficiency, and security. Although, several low-power wireless standards and infrastructure protocols, which try to satisfy such requirements, have been developed, they do not fully comply with them. In the quest to explore possible solutions, the focus is to overcome the existing challenges and explore future research directions. In this paper, we extensively surveyed the existing standards and solutions with main focus on their MAC protocols. We analysed their potentials in satisfying the IWSAN requirements. Our main emphasis was on the industrial control applications because they impose severe challenges. In this regard, the MAC layer can greatly help satisfy such requirements and improve the desired performance metrics. Several MAC protocols have been developed to support general WSN applications but they are not suitable for IWSANs because of the presence of actuator nodes. Therefore, more research efforts and innovative approaches are needed to developing sophisticated protocols so as to seamlessly step into the Industry 4.0.

As a future work, one direction can be to develop a sophisticated MAC scheme to support diverse industrial big data traffic for reliable monitoring and control applications. Another direction is to design a novel communication protocol for reliable and efficient data transmission in diverse industrial applications.

ACKNOWLEDGMENT

The first author would like to thank and acknowledge the financial support of of Pakistan Higher Education Commission (HEC) in collaboration with the German Academic Exchange Services (DAAD) to pursue PhD research.

ORCID

Saleem Raza https://orcid.org/0000-0002-7408-445X
Muhammad Faheem https://orcid.org/0000-0003-4628-4486
Mesut Guenes http://orcid.org/0000-0001-9855-1860

REFERENCES

1. Salarian H, Chin K-W, Naghdy F. Coordination in wireless sensor–actuator networks: a survey. *J Parallel Distrib Comput*. 2012;72(7):856-867.
2. Akyildiz IF, Kasimoglu IH. Wireless sensor and actor networks: research challenges. *Ad Hoc Netw*. 2004;2(4):351-367.
3. Al-Fuqaha A, Guizani M, Mohammadi M, Aledhari M, Ayyash M. Internet of things: a survey on enabling technologies, protocols, and applications. *IEEE Commun Surv Tutorials*. 2015;17(4):2347-2376.
4. Sisinni E, Saifullah A, Han S, Jennehag U, Gidlund M. Industrial internet of things: challenges, opportunities, and directions. *IEEE Trans Ind Inf*. 2018;14(11):4724-4734.
5. Lee J, Bagheri B, Kao H-A. A cyber-physical systems architecture for industry 4.0-based manufacturing systems. *Manuf Letters*. 2015;3:18-23.
6. Fettweis GP. The tactile internet: Applications and challenges. *IEEE Veh Technol Mag*. 2014;9(1):64-70.
7. Oteafy SMA, Hassanein HS. Leveraging tactile internet cognizance and operation via iot and edge technologies. *Proc IEEE*. 2019;107(2):364-375.
8. Park P, Coleri Ergen S, Fischione C, Lu C, Johansson KH. Wireless network design for control systems: A survey. *IEEE Commun Surv Tutorials*. 2018;20(2):978-1013.
9. Özüdoğru AG, Ergün E, Ammari D, Görener A. How industry 4.0 changes business: A commercial perspective. *Int J Commerce Finance*. 2018;4(1):84.
10. Li X, Li D, Wan J, Vasilakos AV, Lai C-F, Wang S. A review of industrial wireless networks in the context of industry 4.0. *Wirel Netw*. 2017;23(1):23-41. https://doi.org/10.1007/s11276-015-1133-7
11. Nikoukar A, Abboud M, Samadi B, Güneş M, Dezfouli B. Empirical analysis and modeling of bluetooth low-energy (ble) advertisement channels. In: 17th Annual Mediterranean ad hoc Networking Workshop (MED-HOC-NET). IEEE; 2018; Capri, Italy:1-6.
12. Nikoukar A, Raza S, Poole A, Güneş M, Dezfouli B. Low-power wireless for the Internet of Things: standards and applications. *IEEE Access*. 2018;6:67893-67926.
13. IEEE Standard for Low-Rate Wireless Networks. IEEE Std 802.15.4-2015 (Revision of IEEE Std 802.15.4-2011) 1–709; 2016.
14. ZigBee Alliance. http://www.zigbee.org/, Last accessed 02-04-2019.
15. Thread Group. http://www.threadgroup.org/, Last accessed 20-05-2019.
16. Z-wave Alliance. http://www.z-wave.com/, Last accessed 21-05-2019.
17. Kushalnagar N, Montenegro G, Schumacher C. Ipv6 over low-power wireless personal area networks (6lowpans):o Overview, assumptions, problem statement, and goals. RFC 4919, RFC Editor; 2007. http://www.rfc-editor.org/rfc/rfc4919.txt
18. LoRa Alliance. https://www.lora-alliance.org/ Last accessed 28-04-2019.
19. FieldComm Group. https://fieldcommgroup.org/, Last accessed 09-05-2018.
20. The International Society of Automation- ISA. https://www.isa.org/, Last accessed 23-01-2019.
21. Industrial Automation Process Automation (WIA-PA). http://www.industrialwireless.cn/en/06.asp, Last accessed 011-09-2018.

22. Ungurean I, Gaitan N, Gaitan VG. An IoT architecture for things from industrial environment. In: 2014 10th International Conference on Communications (COMM); 2014; Bucharest, Romania:1-4.
23. Wang C, Bi Z, Da Xu L. IoT and cloud computing in automation of assembly modeling systems. *IEEE Trans Ind Inf*. 2014;10(2):1426-1434.
24. Åkerberg J, Gidlund M, Björkman M. Future research challenges in wireless sensor and actuator networks targeting industrial automation. In: Proceeding of the international conference on industrial informatics. IEEE; 2011; Caparica, Lisbon, Portugal:410-415.
25. Aazam M, Zeadally S, Harras KA. Deploying fog computing in industrial Internet of Things and Industry 4.0. *IEEE Trans Ind Inf*. 2018;14(10):4674-4682.
26. Wollschlaeger M, Sauter T, Jasperneite J. The future of industrial communication: automation networks in the era of the Internet of Things and Industry 4.0. *IEEE Ind Electron Mag*. 2017;11(1):17-27.
27. Xu LD, Duan L. Big data for cyber physical systems in Industry 4.0: a survey. *Enterp Inf Syst*. 2019;13:148-169.
28. Mrugalska B, Wyrwicka MK. Towards lean production in industry 4.0. *Proc Eng*. 2017;182:466-473.
29. Oliff H, Liu Y. Towards industry 4.0 utilizing data-mining techniques: a case study on quality improvement. *Procedia CIRP*. 2017;63:167-172.
30. Sung TK. Industry 4.0: A Korea perspective. *Technol Forecast Soc Chang*. 2017;132:40-45.
31. Kumar AAS. An industrial perspective on wireless sensor networks a survey of requirements, protocols, and challenges. *IEEE Commun Surv Tutorials*. 2014;16(3):1391-1412.
32. Demirel B. Performance analysis of wireless networked control systems; 2015.
33. Henriksson E. Predictive control for wireless networked systems in process industry. *Ph.D. Thesis*: KTH Royal Institute of Technology; 2014.
34. Liu X, Goldsmith A. Wireless medium access control in networked control systems. In: Proceedings of the 2004 American Control Conference, vol. 4; 2004; Boston, MA, USA, USA:3605-3610. https://doi.org/10.23919/ACC.2004.1384471
35. Rappaport TS. Wireless communications–principles and practice, (the book end). *Microwave J*. 2002;45(12):128-129.
36. Hespanha JP, Naghshtabrizi P, Xu Y. A Survey of recent results in networked control systems. *Proc IEEE*. 2007;95(1):138-162.
37. Abebe ZT. Process control over wireless sensor networks. *Master's Thesis*. KTH Electrical Engineering, Stockholm, Sweden; 2013.
38. Nair GN, Fagnani F, Zampieri S, Evans RJ. Feedback control under data rate constraints: an overview. *Proc IEEE*. 2007;95(1):108-137.
39. Akyildiz IF, Su W, Sankarasubramaniam Y, Cayirci E. A survey on sensor networks. *IEEE Commun Mag*. 2002;40(8):102-105.
40. Faheem M, Abbas MZ, Tuna G, Gungor VC. Edhrp: Energy efficient event driven hybrid routing protocol for densely deployed wireless sensor networks. *J Netw Comput Appl*. 2015;58:309-326.
41. Tuna G, Gungor VC. A survey on deployment techniques, localization algorithms, and research challenges for underwater acoustic sensor networks. *Int J Commun Syst*. 2017;30(17):e3350.
42. Faheem M, Tuna G, Gungor VC. Lrp: Link quality-aware queue-based spectral clustering routing protocol for underwater acoustic sensor networks. *Int J Commun Syst*. 2017;30(12).
43. Römer K. Tracking real-world phenomena with smart dust. In: European Workshop on Wireless Sensor Networks. Springer; 2004; Heidelberg:28-43.
44. Đ*urišić MP, Tafa Z, Dimić G, Milutinović V. A survey of military applications of wireless sensor networks. In: 2012 Mediterranean Conference on Embedded Computing (MECO). IEEE; 2012; Bar, Montenegro:196-199.
45. Wang X, Wang S, Bi D. Distributed visual-target-surveillance system in wireless sensor networks. *IEEE Trans Syst Man Cybern B Cybern*. 2009;39(5):1134-1146.
46. Parra L, Sendra S, Lloret J, Rodrigues JJ. Design and deployment of a smart system for data gathering in aquaculture tanks using wireless sensor networks. *Int J Commun Syst*. 2017;30(16):e3335.
47. Ghayvat H, Mukhopadhyay S, Gui X, Suryadevara N. WSN-and IOT-based smart homes and their extension to smart buildings. *Sensors*. 2015;15(5):10350-10379.
48. Yang L, Ji M, Gao Z, Zhang W, Guo T. Design of home automation system based on Zigbee wireless sensor network. In: 2009 1st International Conference on Information Science and Engineering (ICISE). IEEE; 2009; Nanjing, China:2610-2613.
49. Zanella A, Bui N, Castellani A, Vangelista L, Zorzi M. Internet of Things for smart cities. *IEEE Internet Things J*. 2014;1(1):22-32.
50. Kientopf K, Raza S, Lansing S, Güneş M. Service management platform to support service migrations for IoT smart city applications. In: 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC); 2017; Montreal, QC, Canada:1-5.
51. Jafari R, Encarnacao A, Zahoory A, Dabiri F, Noshadi H, Sarrafzadeh M. Wireless sensor networks for health monitoring. In: The Second Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services, 2005. Mobiquitous 2005. IEEE; 2005:479-481.
52. Mukherjee S, Dolui K, Datta SK. Patient health management system using e-health monitoring architecture. In: 2014 IEEE International Advance Computing Conference (IACC). IEEE; 2014; Palladam, India:400-405.
53. Saneja B, Rani R. An efficient approach for outlier detection in big sensor data of health care. *Int J Commun Syst*. 2017;30(17):e3352.
54. Xu R, Dai H, Jia Z, Qiu M, Wang B. A piecewise geometry method for optimizing the motion planning of data mule in tele-health wireless sensor networks. *Wirel Netw*. 2014;20(7):1839-1858.
55. Dimitrakopoulos G, Demestichas P. Intelligent transportation systems. *IEEE Veh Technol Mag*. 2010;5(1):77-84.
56. Tubaishat M, Zhuang P, Qi Q, Shang Y. Wireless sensor networks in intelligent transportation systems. *Wirel Commun Mob Comput*. 2009;9(3):287-302.

57. Pierce F, Elliott T. Regional and on-farm wireless sensor networks for agricultural systems in eastern Washington. *Comput Electron Agric*. 2008;61(1):32-43.
58. Shen X, Wang Z, Sun Y. Wireless sensor networks for industrial applications. In: Fifth World Congress on Intelligent Control and Automation, 2004. WCICA 2004, Vol. 4. IEEE; 2004; Hangzhou, China, China:3636-3640.
59. Gungor VC, Hancke GP, Member S. Industrial wireless sensor networks : Challenges , design principles , and technical approaches. *IEEE Trans Ind Electron*. 2009;56(10):4258-4265.
60. Zand P, Chatterjea S, Das K, Havinga P. Wireless industrial monitoring and control networks: The journey so far and the road ahead. *J Sens Actuator Netw*. 2012;1(2):123-152.
61. Evers L, Havinga P. Supply chain management automation using wireless sensor networks. In: IEEE International Conference on Mobile ADHOC and Sensor Systems, 2007. MASS 2007. IEEE; 2007; Pisa, Italy:1-3.
62. O'donovan T, Brown J, Büsching F, et al. The ginseng system for wireless monitoring and control: design and deployment experiences. *ACM Trans Sensor Netw (TOSN)*. 2013;10(1):4.
63. Sha K, Shi W, Watkins O. Using wireless sensor networks for fire rescue applications: requirements and challenges. In: 2006 IEEE International Conference on Electro/Information Technology. IEEE; 2006; East Lansing, MI, USA:239-244.
64. ELkamel R, Cherif A. Energy-efficient routing protocol to improve energy consumption in wireless sensors networks. *Int J Commun Syst*. 2017;30(17):1-9.
65. Khan I, Belqasmi F, Glitho R, Crespi N, Morrow M, Polakos P. Wireless sensor network virtualization: early architecture and research perspectives. *IEEE Netw*. 2015;29(3):104-112.
66. Wireless Sensor and Actor Networks (WSAN). http://bwn.ece.gatech.edu/actors/index.html, Last accessed 10-01-2019.
67. Gay D, Levis P, von Behren R, Welsh M, Brewer E, Culler D. The nesc language: a holistic approach to networked embedded systems. In: Proceedings of the ACM SIGPLAN 2003 Conference on Programming Language Design and Implementation, Vol. 38. ACM; 2003; San Diego, California, USA:1-11.
68. Wang Q, Jiang J. Comparative examination on architecture and protocol of industrial wireless sensor network standards. *IEEE Commun Surv Tutorials*. 2016;18(3):2197-2219.
69. Ploplys NJ, Kawka P, Alleyne A. Closed-loop control over wireless networks. *IEEE Control Syst*. 2004;24(3):58-71.
70. Civerchia F, Bocchino S, Salvadori C, Rossi E, Maggiani L, Petracca M. Industrial Internet of Things monitoring solution for advanced predictive maintenance applications. *J Ind Inf Integr*. 2017;7:4-12.
71. Ebert C, Shankar K. Industry trends 2017. *IEEE Softw*. 2017;34(2):112-116.
72. Swain RR, Khilar PM, Dash T. Fault diagnosis and its prediction in wireless sensor networks using regressional learning to achieve fault tolerance. *Int J Commun Syst*. 2018;31(14):e3769.
73. Zhu J, Zou Y, Zheng B. Physical-layer security and reliability challenges for industrial wireless sensor networks. *IEEE Access*. 2017;5:5313-5320.
74. Li B, Ma Y, Westenbroek T, Wu C, Gonzalez H, Lu C. Wireless routing and control: a cyber-physical case study. In: 2016 ACM/IEEE 7th International Conference on Cyber-Physical Systems (IC); 2016; Vienna, Austria:1-10.
75. Park P, Fischione C, Bonivento A, Johansson KH, Sangiovanni-Vincent A. Breath: An adaptive protocol for industrial control applications using wireless sensor networks. *IEEE Trans Mob Comput*. 2011;10(6):821-838.
76. Gunes V, Peter S, Givargis T, Vahid F. A survey on concepts, applications, and challenges in cyber-physical systems. *TIIS*. 2014;8(12):4242-4268.
77. Raza M, Aslam N, Le-Minh H, Hussain S, Cao Y, Khan NM. A critical analysis of research potential, challenges, and future directives in industrial wireless sensor networks. *IEEE Commun Surv Tutorials*. 2018;20(1):39-95.
78. Bachir A, et al. MAC Essentials for Wireless Sensor Networks MAC Essentials for Wireless Sensor Networks. *IEEE Commun Surv Tutorials*. 2010;12(2):222-248.
79. Zhu H, Li M, Chlamtac I, Prabhakaran B. A survey of quality of service in IEEE 802.11 networks. *IEEE Wirel Commun*. 2004;11(4):6-14.
80. Sadeghi R, Barraca JP, Aguiar RL. A survey on cooperative mac protocols in IEEE 802.11 wireless networks. *Wirel Pers Commun*. 2017;95(2):1469-1493.
81. Zhao YZ, Miao C, Ma M, Zhang JB, Leung C. A survey and projection on medium access control protocols for wireless sensor networks. *ACM Comput Surv*. 2012;45(1):7:1-7:37. http://doi.acm.org/10.1145/2379776.2379783
82. Suriyachai P, Brown J, Roedig U. Time-critical data delivery in wireless sensor networks. In: Proceedings of the 6th IEEE International Conference on Distributed Computing in Sensor Systems. Springer-Verlag; 2010; Santa Barbara, CA:216-229.
83. Karl H, Willig A. *Protocols and Architectures for Wireless Sensor Networks*: Wiley; 2006.
84. Akyildiz IF, Vuran MC. *Wireless Sensor Networks*, Vol. 4: John Wiley & Sons; 2010.
85. Muqattash A, Krunz M. CDMA-based mac protocol for wireless ad hoc networks. In: Proceedings of the 4th ACM International Symposium on Mobile ad hoc Networking & Computing. ACM; 2003:153-164.
86. Pompili D, Melodia T, Akyildiz IF. A distributed CDMA medium access control for underwater acoustic sensor networks. In: Proc. of Mediterranean ad hoc Networking Workshop (MED-HOC-NET); 2007:63-70.
87. Tan H-X, Seah WK. Distributed CDMA-based MAC protocol for underwater sensor networks. In: 32nd IEEE Conference on Local Computer Networks, 2007. LCN 2007. IEEE; 2007:26-36.
88. Salajegheh M, Soroush H, Kalis A. Hymac: Hybrid TDMA/FDMA medium access control protocol for wireless sensor networks. In: IEEE 18th International Symposium on Personal, Indoor and Mobile Radio Communications, 2007. PIMRC 2007. IEEE; 2007; Athens, Greece:1-5.

89. Hayajneh M, Khalil I, Gadallah Y. An OFDMA-based MAC protocol for under water acoustic wireless sensor networks. In: Proceedings of the 2009 International Conference on Wireless Communications and Mobile Computing: Connecting the World Wirelessly. ACM; 2009:810-814.
90. Xia F, Rahim A. *MAC Protocols for Cyber-Physical Systems*: Springer; 2015.
91. Abramson N. Development of the ALOHANET. *IEEE Trans Inf Theory*. 1985;31(2):119-123.
92. Doudou M, Djenouri D, Badache N, Bouabdallah A. Synchronous contention-based MAC protocols for delay-sensitive wireless sensor networks: a review and taxonomy. *J Netw Comput Appl*. 2014;38:172-184.
93. Rhee I, Warrier A, Aia M, Min J, Sichitiu ML. Z-mac: A hybrid MAC for wireless sensor networks. *IEEE/ACM Trans Networking*. 2008;16(3):511-524.
94. Sitanayah L, Sreenan CJ, Brown KN. ER-MAC: a hybrid MAC protocol for emergency response wireless sensor networks. In: 2010 Fourth International Conference on Sensor Technologies and Applications (SENSORCOMM). IEEE; 2010:244-249.
95. Hsieh T-H, Lin K-Y, Wang P-C. A hybrid MAC protocol for wireless sensor networks. In: 2015 IEEE 12th International Conference on Networking, Sensing and Control (ICNSC). IEEE; 2015; Taipei, Taiwan:93-98.
96. Ieee standard for local and metropolitan area networks–part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs). IEEE Std 802154-2011 (Revision of IEEE Std 802154-2006) 2011: 1-314. https://doi.org/10.1109/IEEESTD.2011.6012487; 2011.
97. Khanafer M, Guennoun M, Mouftah HT. A survey of beacon-enabled IEEE 802.15. 4 MAC protocols in wireless sensor networks. *IEEE Commun Surv Tutorials*. 2014;16(2):856-876.
98. Anastasi G, et al. A comprehensive analysis of the MAC unreliability problem in IEEE 802.15. 4 wireless sensor networks. *IEEE Trans Ind Inf*. 2011;7(1):52-65.
99. Xia F, Hao R, Cao Y, Xue L. A survey of adaptive and real-time protocols based on IEEE 802.15. 4. *Int J Distrib Sens Netw*. 2011;7(1):11.
100. Pollin S, et al. Performance analysis of slotted carrier sense IEEE 802.15. 4 medium access layer. *IEEE Trans Wirel Commun*. 2008;7(9):3359-3371.
101. Feeney LM, Frey M, Fodor V, Gunes M. Modes of inter-network interaction in beacon-enabled IEEE 802.15.4 networks. In: 2015 14th Annual Mediterranean ad hoc Networking Workshop (MED-HOC-NET); 2015; Vilamoura, Portugal:1-8.
102. Anastasi G, et al. Reliability and energy efficiency in multi-hop IEEE 802.15. 4/Zigbee wireless sensor networks. In: 2010 IEEE Symposium on Computers and Communications (ISCC). IEEE; 2010; Riccione, Italy:336-341.
103. Koubaa A, et al. i-GAME: An implicit GTS allocation mechanism in IEEE 802.15. 4 for time-sensitive wireless sensor networks. In: 18th Euromicro Conference on Real-time Systems, 2006. IEEE; 2006; Dresden, Germany:10-pp.
104. Shrestha B, Hossain E, Camorlinga S, Krishnamoorthy R, Niyato D. An optimization-based GTS allocation scheme for IEEE 802.15. 4 mac with application to wireless body-area sensor networks. In: 2010 IEEE International Conference on Communications (ICC). IEEE; 2010; Cape Town, South Africa:1-6.
105. Na C, Yang Y, Mishra A. An optimal GTS scheduling algorithm for time-sensitive transactions in IEEE 802.15. 4 networks. *Comput Netw*. 2008;52(13):2543-2557.
106. Chen F, et al. Real-time enabled IEEE 802.15. 4 sensor networks in industrial automation. In: IEEE International Symposium on Industrial Embedded Systems, 2009. SIES'09. IEEE; 2009; Lausanne, Switzerland:136-139.
107. Villaverde BC, Alberola RDP, Rea S, Pesch D. Experimental evaluation of beacon scheduling mechanisms for multihop IEEE 802.15.4 wireless sensor networks. In: 2010 Fourth International Conference on Sensor Technologies and Applications (SENSORCOMM). IEEE; 2010; Venice, Italy:226-231.
108. Burda R, Wietfeld C. A distributed and autonomous beacon scheduling algorithm for IEEE 802.15.4/Zigbee networks. In: IEEE International Conference on Mobile ad hoc and Sensor Systems, 2007. MASS 2007. IEEE; 2007; Pisa, Italy:1-6.
109. Jeon H-I, Kim Y. BOP (beacon-only period) and beacon scheduling for MEU (mesh-enabled USN) devices. In: The 9th International Conference on Advanced Communication Technology, Vol. 2. IEEE; 2007; Okamoto, Kobe, Japan:1139-1142.
110. Kim E-J, Choi H-H. EBBS: energy-efficient bop-based beacon transmission scheduling for WSNS. In: IEEE 19th International Symposium on Personal, Indoor and Mobile Radio Communications, 2008. PIMRC 2008. IEEE; 2008; Cannes, France:1-6.
111. Koubaa A, Cunha A, Alves M. A time division beacon scheduling mechanism for IEEE 802.15.4/Zigbee cluster-tree wireless sensor networks. In: Real-time systems, 2007. ecrts'07. 19th euromicro conference on. IEEE; 2007; Pisa, Italy:125-135.
112. Buratti C, Verdone R. Performance analysis of IEEE 802.15.4 non beacon-enabled mode. *IEEE Trans Veh Technol*. 2009;58(7):3480-3493.
113. Huang Y-K, Pang A-C, Hung H-N. A comprehensive analysis of low-power operation for beacon-enabled IEEE 802.15. 4 wireless networks. *IEEE Trans Wirel Commun*. 2009;8(11).
114. Gaglio S, Re GL. *Advances Onto the Internet of Things*, Vol. 260: Springer; 2014.
115. Faridi A, Palattella MR, Lozano A, et al. Comprehensive evaluation of the IEEE 802.15. 4 MAC layer performance with retransmissions. *IEEE Trans Veh Technol*. 2010;59(8):3917-3932.
116. Ramachandran I, Das AK, Roy S. Analysis of the contention access period of IEEE 802.15. 4 MAC. *ACM Trans Sensor Netw (TOSN)*. 2007;3(1):4.
117. Lennvall T, Svensson S, Hekland F. A comparison of WirelessHART and ZigBee for industrial applications; 2008:85-88.
118. Zigbee PRO with Green Power. http://www.zigbee.org/zigbee-for\-developers/network-specifications/zigbeepro/, Last accessed 13-08-2018.
119. Watteyne T, Weiss J, Doherty L, Simon J. Industrial IEEE 802. 15.4 e networks: performance and trade-offs. In: 2015 IEEE International Conference on Communications (ICC). IEEE; 2015:604-609.

120. Dujovne D, Watteyne T, Vilajosana X, Thubert P. 6TiSCH: deterministic IP-enabled industrial internet (of things). *IEEE Commun Mag*. 2014;52(12):36-41.
121. Network D. Technical overview of time synchronized mesh protocol; 2006.
122. Pister KSJ, Doherty L. TSMP: Time synchronized mesh protocol. In: 20th, IASTED international conference on parallel and distributed computing and systems; 2008; Orlando, FL:391-398.
123. De Guglielmo D, Seghetti A, Anastasi G, Conti M. A performance analysis of the network formation process in IEEE 802.15.4e TSCH wireless sensor/actuator networks. In: 2014 IEEE Symposium on Computers and Communication (ISCC). IEEE; 2014; Funchal, Portugal:1-6.
124. Kurunathan H, Severino R, Koubaa A, Tovar E. Towards worst-case bounds analysis of the IEEE 802.15. 4e. In: 22nd IEEE Real-time Embedded Technology & Applications Symposium Work in Progress Session. Institute of Electrical and Electronics Engineers; 2016; Vienna, Austria.
125. Alderisi G, Patti G, Mirabella O, Bello LL. Simulative assessments of the IEEE 802.15. 4e DSME and TSCH in realistic process automation scenarios. In: 2015 IEEE 13th International Conference on Industrial Informatics (INDIN). IEEE; 2015; Cambridge, UK:948-955.
126. Vilgelm M, Gürsu M, Zoppi S, Kellerer W. Time slotted channel hopping for smart metering: measurements and analysis of medium access. In: 2016 IEEE International Conference on Smart Grid Communications (SMARTGRIDCOMM); 2016; Sydney, NSW, Australia:109-115.
127. Yaala SB, Bouallegue R. On mac layer protocols towards internet of things: from IEEE 802.15.4 to IEEE 802.15.4e. In: 2016 24th International Conference on Software, Telecommunications and Computer Networks (SOFTCOM); 2016; Split, Croatia:1-5.
128. Elsts A, Fafoutis X, Pope J, Oikonomou G, Piechocki R, Craddock I. Scheduling high-rate unpredictable traffic in IEEE 802.15. 4 TSCH networks. In: 2017 13th International Conference on Distributed Computing in Sensor Systems (DCOSS); Ottawa, ON, Canada:3-10.
129. Palattella MR, Accettura N, Grieco LA, Boggia G, Dohler M, Engel T. On optimal scheduling in duty-cycled industrial IoT applications using IEEE 802. 15.4 e TSCH. *IEEE Sensors J*. 2013;13(10):3655-3666.
130. Palattella MR, Accettura N, Dohler M, Grieco LA, Boggia G. Traffic aware scheduling algorithm for reliable low-power multi-hop IEEE 802.15. 4e networks. In: 2012 IEEE 23rd International Symposium on Personal Indoor and Mobile Radio Communications (PIMRC). IEEE; 2012; Sydney, NSW, Australia:327-332.
131. Accettura N, Palattella MR, Boggia G, Grieco LA, Dohler M. Decentralized traffic aware scheduling for multi-hop low power lossy networks in the internet of things. In: 2013 IEEE 14th International Symposium and Workshops on a World of Wireless, Mobile and Multimedia Networks (WOWMOM). IEEE; 2013; Madrid, Spain:1-6.
132. Hwang R-H, Wang C-C, Wang W-B. A distributed scheduling algorithm for IEEE 802.15. 4e wireless sensor networks. *Comput Stand Interfaces*. 2017;52:63-70.
133. Soua R, Minet P, Livolant E. DiSCA: A distributed scheduling for convergecast in multichannel wireless sensor networks. In: 2015 IFIP/IEEE International Symposium on Integrated Network Management (IM). IEEE; 2015:156-164.
134. Soua R, Minet P, Livolant E. Wave: a distributed scheduling algorithm for convergecast in IEEE 802.15.4e TSCH networks. *Trans Emerg Telecommun Technol*. 2016;27(4):557-575.
135. Kim KT, Kim H, Park H, Kim S-T. An industrial IoT MAC protocol based on IEEE 802.15. 4e TSCH for a large-scale network. In: 2017 19th International Conference on Advanced Communication Technology (ICACT). IEEE; 2017; Bongpyeong, South Korea:721-724.
136. De Guglielmo D, Brienza S, Anastasi G. A model-based beacon scheduling algorithm for IEEE 802.15.4e TSCH networks. In: 2016 IEEE 17th International Symposium on a World of Wireless, Mobile and Multimedia Networks (WOWMOM). IEEE; 2016; Coimbra, Portugal:1-9.
137. van der Lee T, Raza S, Exarchakos G, Güneş M. Towards co-located TSCH networks: an inter-network interference perspective; 2018:1-6.
138. Yaala SBen, Théoleyre F., Bouallegue R. Performance study of co-located IEEE 802.15.4-TSCH networks: interference and coexistence. In: 2016 IEEE Symposium on Computers and Communication (ISCC); 2016; Messina, Italy:513-518.
139. Watteyne T, Palattella M, Grieco L. Using IEEE 802.15.4e time-slotted channel hopping (TSCH) in the internet of things (IoT): problem statement. RFC 7554, RFC Editor; 2015.
140. Internet Engineering Task Force. https://www.ietf.org/. Last accessed 02-07-2018.
141. Wang Q, Vilajosana X, Watteyne T. 6TiSCH operation sublayer (6top) draft-wang-6tisch-6top-sublayer-01. tech. rep., Internet-Draft. IETF; 2014.
142. Willig A, Matheus K, Wolisz A. Wireless technology in industrial networks. *Proc IEEE*. 2005;93(6):1130-1151.
143. Scheible G, Dzung D, Endresen J, Frey JE. Unplugged but connected—design and implementation of a truly wireless real-time sensor/actuator interface. *IEEE Indust Electron Mag*. 2007;1(2):25-34.
144. Song J, Han S, Mok AK, et al. WirelessHART: Applying wireless technology in real-time industrial process control,; 2008:377-386.
145. Mavromoustakis C, Mastorakis G, Batalla JM. *Internet of Things (IoT) in 5G Mobile Technologies*, Vol. 8: Springer; 2016.
146. Christin D, et al. Survey on wireless sensor network technologies for industrial automation: the security and quality of service perspectives. *Future Int*. 2010;2(2):96-125.
147. Rezha FP, Shin SY. Performance evaluation of ISA100. 11A industrial wireless network. In: IET International Conference on Information and Communications Technologies (IETICT 2013); 2013; Beijing, China, China:587-592.
148. Costa MS, Amaral JL. Analysis of wireless industrial automation standards: Isa-100.11 a and wirelesshart. InTech Magazine; 2012.
149. Petersen S, Carlsen S. WirelessHART versus ISA100.11a: the format war hits the factory floor. *IEEE Ind Electron Mag*. 2011;5(4):23-34.
150. Chinese Industrial Wireless Alliance (CIWA). http://www.industrialwireless.cn/en/06.asp, Last accessed 29-09-2018.
151. International Electrotechnical Commission (IEC). http://www.iec.ch/, Last accessed 01-10-2018.

152. Liang W, Zhang X, Xiao Y, Wang F, Zeng P, Yu H. Survey and experiments of WIA-PA specification of industrial wireless network. *Wirel Commun Mob Comput*. 2011;11(8):1197-1212.
153. Wang H, Wei X, Wang P. A transmission scheme of IPv6 packets over WIA-PA networks. In: Chinese Automation Congress (CAC), 2015. IEEE; 2015; Wuhan, China:1137-1142.
154. Zurawski R. *Industrial Communication Technology Handbook*: CRC Press; 2014.
155. Shen W, Zhang T, Barac F, Gidlund M. Prioritymac: A priority-enhanced mac protocol for critical traffic in industrial wireless sensor and actuator networks. *IEEE Trans Ind Inf*. 2014;10(1):824-835.
156. Suriyachai P, et al. Implementation of a MAC protocol for QoS support in wireless sensor networks. In: IEEE International Conference on Pervasive Computing and Communications, 2009. PERCOM 2009. IEEE; 2009; Galveston, TX, USA:1-6.
157. Zheng T, Gidlund M, Åkerberg Johan. Wirarb: A new mac protocol for time critical industrial wireless sensor network applications. *IEEE Sensors J*. 2016;16(7):2127-2139.
158. Somappa AAK, Øvsthus K, Kristensen LM. Towards a dual-mode adaptive MAC protocol (DMA-MAC) for feedback-based networked control systems. *Proc Comput Sci*. 2014;34(C):505-510.
159. Jeschke S, Brecher C, Meisen T, Özdemir D., Eschert T. Industrial internet of things and cyber manufacturing systems. *Industrial Internet of Things*: Springer; 2017:3-19.
160. Li J, Yu FR, Deng G, Luo C, Ming Z, Yan Q. Industrial internet: a survey on the enabling technologies, applications, and challenges. *IEEE Commun Surv Tutorials*. 2017;19:1504-1526.
161. Geissbauer R, Vedso J, Schrauf S. Industry 4.0: building the digital enterprise: 2016 global industry 4.0 survey. PwC, Munich; 2016.
162. Raza U, Kulkarni P, Sooriyabandara M. Low power wide area networks: an overview. *IEEE Commun Surv Tutorials*. 2017;19(2):855-873.
163. Bash E. Real-time mesh network for industrial automation. 2015;1. arXiv:1011.1669v3.
164. Palattella MR, Watteyne T, Wang Q, et al. On-the-fly bandwidth reservation for 6TiSCH wireless industrial networks. *IEEE Sens J*. 2016;16(2):550-560.
165. Li W, Privat G, Le Gall F. Towards a semantics extractor for interoperability of IoT platforms. In: Global Internet of Things Summit (GIOTS), 2017. IEEE; 2017; Geneva, Switzerland:1-6.
166. Ganzha M, Paprzycki M, Pawłowski W, Szmeja P, Wasielewska K. Semantic interoperability in the internet of things: an overview from the inter-IoT perspective. *J Netw Comput Appl*. 2017;81:111-124.
167. Babulal KS, Tewari RR. Cross layer design for cooperative transmission in wireless sensor networks. *Wirel Sens Netw*. 2011;3(6):209.
168. Vuran MC, Akyildiz IF. Xlp: A cross-layer protocol for efficient communication in wireless sensor networks. *IEEE Trans Mob Comput*. 2010;9(11):1578-1591.
169. Van Hoesel L, Nieberg T, Wu J, Havinga PJ. Prolonging the lifetime of wireless sensor networks by cross-layer interaction. *IEEE Wirel Commun*. 2004;11(6):78-86.
170. Radmand P, Talevski A, Petersen S, Carlsen S. Taxonomy of wireless sensor network cyber security attacks in the oil and gas industries,; 2010:949-957.
171. Chen D, Nixon M, Mok A. Why wirelesshart. *Wirelesshart*: Springer; 2010:195-199.
172. Walters JP, Liang Z, Shi W, Chaudhary V. *Wireless Sensor Network Security: A Survey*, Vol. 367. Boca Raton, FL, USA: CRC Press; 2007.
173. Wang Y, Attebury G, Ramamurthy B. A survey of security issues in wireless sensor networks. *IEEE Commun Surv Tutorials*. 2006;8(2):2-23.
174. Chen X, Makki K, Yen K, Pissinou N. Sensor network security: A survey. *IEEE Commun Surv Tutorials*. 2009;11(2):52-73.

How to cite this article: Raza S, Faheem M, Guenes M. Industrial wireless sensor and actuator networks in industry 4.0: Exploring requirements, protocols, and challenges—A MAC survey. *Int J Commun Syst*. 2019;32:e4074. https://doi.org/10.1002/dac.4074