An Industrial Perspective on Wireless Sensor Networks — A Survey of Requirements, Protocols, and Challenges

A. Ajith Kumar S., Knut Øvsthus, and Lars M. Kristensen.

***Abstract*—Wireless Sensor Networks (WSNs) are applicable in numerous domains, including industrial automation where WSNs may be used for monitoring and control of industrial plants and equipment. However, the requirements in the industrial systems differ from the general WSN requirements. In recent years, standards have been defined by several industrial alliances. These standards are specified as frameworks with modifiable parts that can be defined based on the particular application of WSN. However, limited work has been done on defining industry-specific protocols that could be used as a part of these standards. In this survey, we discuss representative protocols that meet some of the requirements of the industrial applications. Since the industrial applications domain in itself is a vast area, we divide them into classes with similar requirements. We discuss these industrial classes, set of common requirements and various state-of-the-art WSN standards proposed to satisfy these requirements. We then present a broader view towards the WSN solution by discussing important functions like medium access control, routing, and transport in detail to give some insight into specific requirements and the classification of protocols based on certain factors. We list and discuss representative protocols for each of these functions that address requirements defined in the industrial classes. Security function is discussed in brief, mainly in relation to industrial standards. Finally, we identify unsolved challenges that are encountered during design of protocols and standards. In addition some new challenges are introduced and discussed.**

***Index Terms*—Wireless Sensor and Actuator Networks, Industrial automation, Standards, Medium Access Control, Routing, Transport, Security.**

I. Introduction

A WIRELESS sensor network (WSN) is a network of micro-electro-mechanical systems (MEMS) [1] called sensor devices deployed to gather sensory information from an area of interest. Sensor devices (nodes) have the ability to sense, process, and communicate data. These devices typically have limited computing power and are designed to operate on batteries. Initially, these sensor devices were used in military applications [2]. Technological advances in the area of wireless communication, sensors, and batteries have opened up many new prospects for applications [3], [4] and research. Currently, these devices are extensively used for realizing smart environments with automation of control systems and are also finding various applications in the area of smart homes, transportation, industrial automation, and health-care monitoring.

In this article, we focus on the use of WSN in industrial applications [5] also referred to as Industrial Wireless Sensor Networks (IWSN). We specifically consider industrial applications for control systems, which are different from the conventional control systems [6]. The industrial segment is an ever growing sector and huge amounts of capital are invested on research activities to support the advancements in WSN technology. In an industrial scenario, the aim is to use these low-power, low cost nodes reducing the CAPital EXpenditure (CAPEX) and Operational EXpenditure (OPEX) [7] of the network significantly compared to the wired networks without loss in quality of service (QoS). The use of IWSN in observing more and more parameters in the production cycle and obtaining valuable feedbacks increases productivity and efficiency of the industrial applications. The important features of IWSN are: self-organization, easy-deployment, low-maintenance, and robust operation.

A general centralized IWSN scenario is depicted in figure 1 with nodes, sink/network manager, management console, and process controllers. The nodes collect data and communicate it to the sink/network manager which in turn communicates this data to the process controller. The nodes are managed by the network manager and the network manager can be controlled via a management console. The black arrows show a path through which a sensor node at the far end communicates to the sink via other nodes. In the control automation segment of the industry, the use of WSN as a part of the control loop has given rise to new possibilities. In these types of networks, the process controllers (actuators) are a part of the sensor network as shown in figure 2. The nodes communicate data directly to the actuators (dashed arrows) and the actuators may also have some communication among themselves (solid arrows). These networks are referred to as wireless sensor and actuator (actor) networks (WSAN) [8], [9]. The actuators are used to operate units e.g. a valve and this is done based on the data sent by the sensors e.g. temperature and pressure. WSAN is a subclass of IWSN as discussed in section II. With the use of WSAN, the entire control loop can be automated, saving largely on CAPEX and OPEX.

There are various wireless standards proposed to be used in IWSN, most importantly, Zigbee [10], ISA100.11a [11], WIA-

Manuscript received February 28, 2013; revised October 16, 2103.

A. Kumar is with the Faculty of Engineering, Bergen University College and the Faculty of Engineering and Science, University of Agder. (e-mail: aaks@hib.no)

K. Øvsthus and L. M. Kristensen are with the Faculty of Engineering, Bergen University College, Bergen, Norway. (e-mail: {kovs,lmkr}@hib.no)

Digital Object Identifier 10.1109/SURV.2014.012114.00058

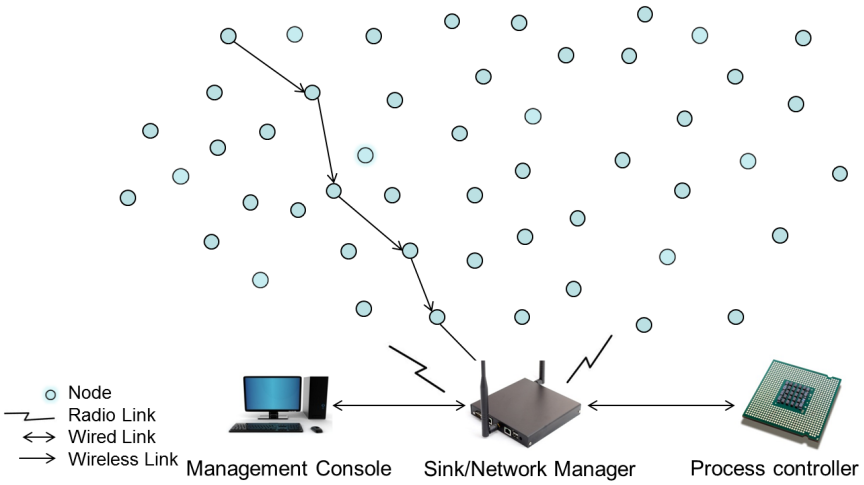

Fig. 1. General IWSN

PA [12], and wirelessHART [13]. These standards are used in various IWSN applications and are designed like frameworks that can be customized to the needs of a particular application setting, since they are not strictly defined at each *layer* of the communication protocol stack. The term *Layer* we refer to is in accordance to the Open Systems Interconnection (OSI) model.

A WSN node consists of three main components: the processing unit, the communication unit, and the sensor unit. In this article, we abstract from the sensor part and focus on the communications unit, especially on the Medium Access Control(MAC), routing, and transport functions. Security function is also discussed briefly in relation to the industrial standards. In the literature, there is a debate whether WSN should replicate the layered structure of the Internet or if it should have a more flexible design [14]. Taking routing as an example, there is a debate where it should be implemented, in the network layer or in the MAC layer [15]. Many research articles that we surveyed are generic and do not specify which layer they are addressing. This article does not take part in the discussion of where for example routing should be implemented, but we recognize that a routing function is required. Also, these functions can be provided at different layers via cross-layer communication. Hence, we preferably refer to them as functions rather than referring to them as layers that are known to provide them.

Among the two units we focus on (computing and radio communication), the latter consumes the most energy in the nodes [16], [17]. The MAC function is responsible for the medium access which controls most of the radio communication; hence it plays a vital role in increasing the energy efficiency and also in decreasing latency. Other functions like the routing function can considerably affect the energy efficiency [18], latency, and reliability. Transport protocols in WSNs are responsible for congestion control and loss recovery [19], with the aim of providing end-to-end packet delivery and hence increase reliability. We go through MAC, routing, and transport functions, and discuss how the functions can be realized taking into account the IWSN requirements.

There exists already various surveys on WSN [20], [4] that describe protocols proposed for various layers, key challenges in WSN, hardware, test-beds used, and applications for these WSN. There are other surveys which focus on specific layers or functions like *Medium Access Control*(MAC) [21], [22], [23], [24], *routing* [18], [25], [26], and *transport* functions [19], [27]. Recent surveys also focus on a particular service provided by the protocols under a given function, e.g. application-oriented MAC protocols [28], [29]. On the other end, we have surveys on IWSN [30], [31], [32] focusing on challenges, design principles, technical approaches to build IWSN, their requirements, WSN standards, and QoS. The article [33] combines some protocols and mechanisms to satisfy requirements like reliability, latency, and real-time operation but is limited to MAC and routing functions. In comparison with these survey articles, the contribution of this article is to:

- View the WSN domain in an industrial perspective and put every detail discussed here into this context. We discuss the classification of industrial applications into certain classes with application examples. The industrial systems with common requirements and goals are grouped into a single class.
- Review the list of important requirements set by industrial applications discussed previously and add-in certain less treated requirements in WSN that relates more to WSAN (e.g., Multiple source and multiple sinks, predictable behaviour). In addition, we also review state-of-the-art in industrial standards along with a new solution (GinMAC).
- Concentrate on three important functions: MAC, routing and transport. Each of these functions is discussed in detail along with design requirements specific to industrial systems to be considered when designing these functions. In addition to these, security is treated in brief with focus on how industrial wireless standards implement it.
- Present representative protocols for MAC, routing and transport function that are picked after carefully reviewing various protocols in the same class, and do meet most or all of the industrial requirements.

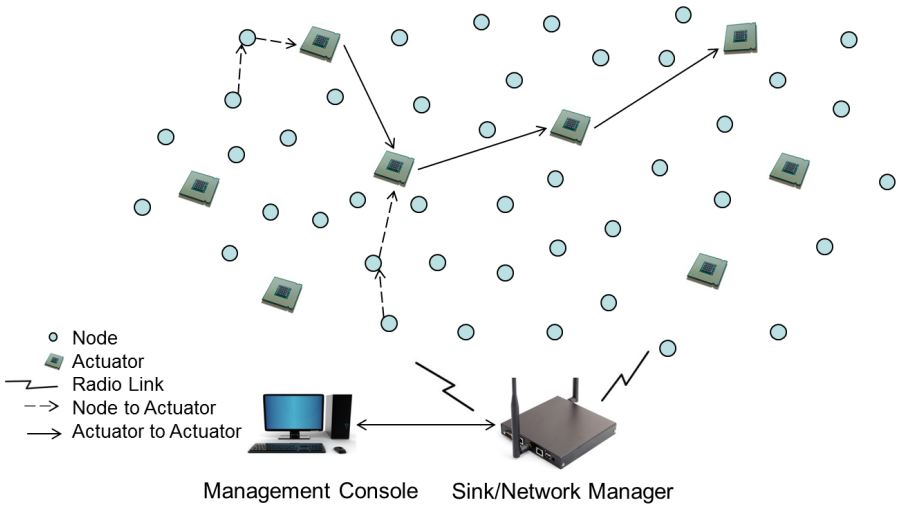

Fig. 2. Wireless Sensor Actuators Networks

- Review important recent challenges involved in the design of protocols for this domain and add in some new points that we consider important and related to this domain. Also, we summarize the classes of industrial systems via mapping of representative protocols to the identified classes of systems by particular class.

The remainder of the article is divided into seven sections. We start by briefly describing the context of IWSN in section II, the classes of systems we focus on, the design requirements of these classes of systems, and state-of-the-art industrial standards defined in recent years. A brief introduction of the security function in IWSN along with some details on security features provided by the industrial standards is presented in section III. We then describe the functions we focus on. In section IV we discuss medium access control, in section V we discuss routing functions, and in section VI we discuss transport functions. Based on the discussion of the MAC, routing and transport functions, and the experience gained from the study, we then identify the current challenges in the design of IWSN in section VII. Finally, we give a summary of our study by identifying the protocols that are applicable to the industrial classes of systems considered and conclude in section VIII.

II. Industrial WSN, Applications, Requirements and Standards

IWSN is different from traditional WSN in terms of their requirements. Also, IWSN is a vast domain, and it has therefore been divided into classes depending on functional and on service requirements. In this section we discuss the classification of industrial systems, applications of WSN in such systems, provide important industrial design requirements, and present state-of-the art standards that have been proposed.

A. Industrial WSN

According to the International Society of Automation, the industrial systems can be classified into six classes [33], [34] based on criticality of data and operational requirements. These classes range from critical control systems to monitoring systems, and their operational requirements and criticality vary accordingly. These six classes are:

- *Safety systems*. Systems where immediate (in the order of ms or s) action on events is required in the order of seconds, belong to this class e.g. fire alarm systems. The WSN nodes are deployed uniformly throughout the area of concern to cover the entire area. The nodes are usually stationary.
- *Closed loop regulatory systems*. Control system where feedbacks are used to regulate the system. WSN nodes are deployed in the area of concern in a desired topology. Periodically and based on events, measurements are sent to the controller. Periodic measurements are critical for the smooth operation of the system. These systems may have timing requirements that are stricter than safety systems. Based on these measurements, controller makes a decision and sends it to the actuators which act on this data. Due to its strict requirements, a new protocol suite is proposed for this class of systems [35]. A simple control loop with wireless sensors and an actuator is shown in figure 3.
- *Closed loop supervisory systems*. Similar to regulatory systems with the difference that feedbacks/measurements are not expected periodically but can be based on certain events. The feedbacks are non-critical e.g. a supervisory system that collects statistical data and reacts only when certain trends are observed, which can be related to an event.
- *Open loop control systems*. Control systems operated by a human operator, where a WSN is responsible for data collection and relaying the collected data to the central database. The operator analyzes this data and undertakes any measures if required.
- *Alerting systems*. Systems with regular/event-based alerting. An example is a WSN for continuous monitoring of temperature in a furnace and alerting at different stages, to indicate part of the work done.
- *Information gathering systems*. System used for data col-

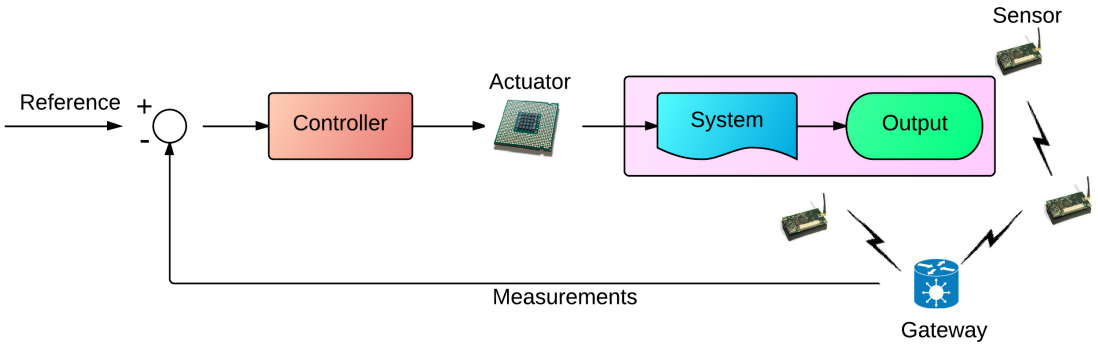

Fig. 3. Wireless closed loop control with sensors and actuators

lection and data forwarding to a server. An example could be WSN nodes deployed in a field to gather data about the area of interest, such as temperature and moisture, for a specific duration of time. This data gathered over a long period can then be used to decide on long term plans for managing temperature and moisture.

The alert function in a temperature monitoring system is primarily non-critical, to just alert at different measures of temperature to indicate completion of certain processes. But when the temperature goes beyond a certain level, the alerting system might be required to act as a safety system. Thus some classes of systems are sometimes expected to play more than one role.

B. Industrial Applications

WSN are used in wide range of applications in the industrial domain [36] and eliminates the requirement of human presence in various places including dangerous areas to obtain sensory information and actuation control. This also reduces the cost for the industry which used wired solutions previously, since wiring involves a premium cost [37]. Wiring also could incur additional costs of using insulation to be protected from various harmful physical effects such as high temperature. It is also a problem when existing system solution installations have to be replaced or removed, the wiring placements also have to be replaced or moved around. Also, movable objects pose a great challenge to implement wiring around it, as it restricts its movability, for example a robot. Wireless devices are advantageous in all these cases where the only requirement is for the device to be insulated for withstanding extreme conditions. The classes of systems defined previously can also be seen as three categories: safety systems, control systems, and monitoring systems. Below we discuss some of the applications, in each of these categories. Various other applications for which WSN is used can be found in [3], [4].

Safety systems. Fire safety [38] is one of the important safety systems WSN has been applied. WSN ensures its applicability to safety systems by providing various features like real-time monitoring, close monitoring of fire fighters (or early responders like police, medic etc) and web-enabled service to provide real-time information to staff standby outside the disaster site. The real-time monitoring assists in keeping the fire-fighters informed. On the industrial perspective, WSN is used in safety systems in potentially dangerous applications like nuclear power plants [39], [40]. Mainly, the problems imposed are due to aging of the components used in these plants, which goes undetected without proper monitoring.

Control systems. One of the main categories of the industrial application of wireless sensor networks is the control systems. Firstly, the closed loop control systems [41] which are mainly used to monitor various devices in the system and act accordingly when changes are observed. These closed loop control systems can be further classified into: process control systems and factory automation systems [33]. Process control systems usually are based on monitoring and actuation with delay requirements ($<$100ms) that are not as strict as factory automation systems (for example 2-50 ms as in Robot control [33]). Secondly, open loop control systems [42] are similar to closed loop control with the extra feature of having human in the loop to supervise the control actions.

Monitoring systems. The last two classes, alerting systems and information gathering systems are systems that have been using traditional WSN with minimum requirements. A wide range of applications are served by these systems [4], [43], [44] including environmental monitoring, industrial monitoring, traffic monitoring and also military applications. These systems are basically used to collect data over a given area for a long duration and this data is studied thoroughly to arrive at certain conclusions.

C. IWSN Requirements

Wireless standards designed for IWSN are expected to satisfy various requirements specific to the industrial domain. Below we discuss these requirements in brief.

- *Minimal Cost and Compactness*. Industrial WSN aim at increased productivity, decreased cost and increased profit. Lower cost requirements for deployment and implementation are the prime motivations that drive the transition from the use of wired solutions to wireless solutions. The wired solutions are rated at $200 per sensor according to [37]. The smaller sizes of the wireless nodes have added to its advantages in decreasing space requirements for installation in addition to its cost savings. Thus IWSN solutions are expected to reduce cost and have wireless nodes of compact sizes. The compact size also aids in easing the installation of large-scale network of nodes.

- *Interoperability*. Current industries already use wired systems with sensors for various measurements and operations. The use of new wireless solutions needs to cooperate with these legacy systems. Interoperability is also required with other wireless solutions that could be used for some specific purpose.
- *Resistance to Noise and Co-existence*. WSN operate on low-power signals and are highly susceptible to noise. A typical industrial site contain various wireless networks, machineries and communication systems that can create interference [45], [46] to the radio signals increasing the path loss. The WSN standards are expected to efficiently withstand the interference and work efficiently in its presence. These co-existence issues in the Industrial-Scientific-Medical (ISM) band between various wireless networks operating at 2.4 GHz have also been studied and confirmed [47].
- *Energy consumption*. This requirement can be considered in two dimensions: *low energy consumption* and *efficient energy consumption*. Concerning *low energy consumption*, the WSN nodes are commonly powered by batteries and the nodes are required to be energy efficient to ensure a longer lifetime of the network. The use of low-power signals contributes to increasing the energy efficiency. Concerning *efficient energy consumption*, the WSN consists of several nodes and hence to increase the energy efficiency of the entire network, the load over the network has to be balanced. Energy-aware management techniques and routing protocols are essential for load balancing and thus increasing the overall lifetime of the network.
- *Self-organizing*. WSNs are built to be self-configuring and self-organizing. In the context of IWSN, the sensor nodes are usually placed in strategic locations that may not be easily accessible. They are thus required to operate independent of human intervention for long durations of time. Thus autonomous operation is one of the major requirements. Examples are, WSN nodes deployed in harsh conditions like extreme cold climates or near huge machines operating at high temperatures.
- *Robustness/Fault-Tolerance*. In-line with the previous requirement, WSN is expected to be fault-tolerant and robust against failures. Given the limited energy, sensor nodes stop to operate after a certain duration of time. The network should be built such that failure of one or a few sensor nodes does not result in failure of the entire network. Thus robust routing protocols are required which are responsive to dynamic changes in topology.
- *Link-Reliability*. Low powered WSN nodes have relatively low link reliability compared to traditional wireless networks. This leads to high packet loss and high delay, rendering the WSN unusable in the industrial context. Measures need to be taken to overcome the link failures using efficient retransmission techniques at the link layer, the transport layer or using replication based routing protocols [48].
- *Low-delay*. Among the various classes of systems, the control systems are delay sensitive systems. Specifically, the closed loop regulatory systems are extremely delay sensitive and require the WSN communication to have predictable behaviour and expect real-time guarantees.
- *Service Differentiation*. IWSNs are complex systems consisting of a combination of different type of sensors. Different classes of data generated from these sensors often require different treatment in the network and thus require service differentiation. Service differentiation can be at different levels e.g., node level, packet level, and can also be spatially different. Also, within similar sensor nodes, some sensed values are more important than others, e.g. values beyond some threshold could be important. This service differentiation is implemented by assigning priorities. For node level priority, different types of nodes are given different priority. Service differentiation is a prime requirement in the case of WSAN, since actor to actor communication is different from sensor to sensor communication or sensor to actor communication.
- *Quality of Service*(QoS). IWSNs are application oriented and each application may vary in its specific requirements. The requirements can also be specified in terms of service requirements with minimum required quality mentioned explicitly, which then determines the Quality of Service. For example, data has to be transferred between two points in a network within 25ms. Applications impose specific requirements for each function in the communication system which can be viewed separately at each function. Chen et al. [49] defines two perspectives; *application specific QoS* and *network QoS*. *Application specific QoS* is a higher level abstraction of QoS requirements at the application level. Minimum coverage area, minimum number of active sensors and measurement precision could be considered as *application specific QoS*. *Network QoS* represents a lower level perspective at the more detailed communication part, where the QoS required by the data packets are considered. Reliability, latency, and availability are some of the major *network QoS* requirements. The first four classes of systems defined in section II have strict QoS requirements. QoS is a common requirement and has to be considered in each function.
- *Scalability*. Scalability can be viewed from two different perspectives. First we see it from the design perspective of protocols and standards, which need to be scalable in order to match different requirements of industrial applications. On the second perspective, industries evolve with time and thus the IWSN installations need to be scalable to adapt to these changes to allow for addition or removal of numerous sensor nodes. With time, new functionalities have to be supported which would need sensor nodes in the order of hundreds of nodes for each function. This is a common requirement for large industries since WSN installations are expected to run for long duration of time. Thus IWSN needs to be scalable enough to accommodate these new nodes without degradation in *QoS*. The self-organizing requirement is also essential for scalability.
- *Multiple source and multiple sinks*. With the continuous advancement in the WSN hardware and software, the possibility to use multiple applications across a single WSN has increased. A possible topological difference

due to this change is the use of multiple sinks [50] in a single network. One example for such topology is WSAN networks which have multiple actors which can act as separate sinks. This multiple applications scenario is a common scenario in complex industrial systems. Hence, designing routing solutions for multiple source and multiple sink scenarios is an important requirement in IWSN.

- *Predictable Behaviour*. Industrial systems are large and complex systems, and these systems impose a set of requirements that have to be realized. Thus solutions are required to have predictable behaviour in order to ensure that the requirements are realized efficiently. With such complexity, huge costs are involved and any solution proposed is required to be analyzable before installation and implementation in order to assure that a correct solution is being used. Thus trustworthy solutions are needed for IWSN, especially for WSAN [29].
- *Application Specific Protocols*. IWSN standards could be re-usable in various application scenarios but the protocols used within these standards are dominantly targeting specific applications. Different industrial applications have different requirements, and hence there is a need for specific protocols satisfying the corresponding requirements.
- *Data Aggregation*. Sensors sense data continuously and this consecutively sensed data may be redundant. Also, sensors deployed in a particular area might sense similar or identical data. The importance of this sensed data depends on the application requirements, and for some applications it might be sufficient to get aggregated results from these sensors. Data aggregation can either be of data in the same sensor or from a group of sensors. This increases energy efficiency by minimizing the number of packets sent. This is more of an application layer function.

For more information on IWSN requirements, challenges and technical approaches see Gungor et al. [30]. Apart from general IWSN requirements, industrial WSN being more focused on real implementations expect proposed protocols to be based on realistic assumptions. One study discussing general misconceptions regarding timeliness in WSN is Oliver et al. [51]. Due to unavailability of time and resources, it is also common to propose a protocol design and simulate it over various available network simulators [52] to prove its usefulness. Alternatively, performance modelling and analysis could be done analytically. These analytical models could be slightly pessimistic [53], [54] owing to various assumptions made due to the complex nature of the system. Such proposals might not be accurate due to inaccuracy existing in the simulation models or simulators [55], [56], [57]. Thus eventual implementation, deployment and real-world testing is essential for the proper evaluation of protocols proposed for IWSN.

D. Industrial Standards

IWSN are required to have some basic qualities: low-power, high reliability, and easy deployment, administration, and maintenance. These basic requirements drive the design goals for these devices. Various working groups like the Wireless Networking Alliance (WINA) [58], the Zigbee Alliance [59], the HART Communication Foundation (HCF) [60], the International Society of Automation [61], and the Chinese Industrial Wireless Alliance [12] have established standards for IWSN [43]. The resulting standards are wirelessHART [13], ZigBee [10], ISA100.11a [11], and WIA-PA [12] which are all based on the IEEE 802.15.4 standard. We also discuss the GINSENG project [62] which is not in itself a wireless standard, but is developed as a solution for performance control in closed loop control systems using WSN. In this article, we discuss wirelessHART, ISA100.11a, WIA-PA, and the GINSENG project. These are all based on Time Division Multiple Access(TDMA) due to the advantages that TDMA has over Carrier Sense Multiple Access(CSMA) as will be discussed in section IV-A.

WirelessHART. This standard is based on the IEEE 802.15.4 physical layer, with an operation frequency of 2.4GHz and uses 15 different channels. It uses the Time Synchronized Mesh Protocol (TSMP) [63] which was developed by Dust Networks [64] for medium access control and network layer functions. TSMP uses TDMA for channel access and allows for channel hopping and channel blacklisting at the network layer. Channel hopping is a technique in which data transfer happens at different frequencies at different periods of time. The wirelessHART standard supports up to 15 channels which are used in turns. Channel blacklisting is a process of blacklisting channels which exhibit large interference with the signals. This use of TDMA with channel hopping and channel blacklisting has decreased the effect of interference and noise. WirelessHART supports redundant routing in order to enhance reliability. WirelessHART is thus considered to be robust, energy efficient and reliable, but since this is still an emerging standard, there is a lot of scope for improvement. WirelessHART was designed, developed and standardized with industrial systems in mind and supports legacy systems built on wired HART. The network topologies supported by the network manager in wirelessHART are *Star* and *Mesh*.

ISA100.11a. The ISA100 working group developed this standard in order to provide robust and secure communication for applications in process automation [65]. Similar to wirelessHART, the physical layer is based on IEEE 802.15.4. ISA100.11a also uses channel hopping and channel blacklisting to reduce interference effects. ISA100.11a applies different methods for channel hopping like *slow hopping*, *fast hopping*, and *mixed hopping*. At the data link layer, it combines TDMA with CSMA in order to capitalize on the advantages in both solutions. At the network layer, the compatibility with IPv6 gives opportunities for users to connect to the Internet, thus providing diverse possibilities. The ISA standard supports integration with legacy protocols like wired HART. ISA also provides interface for and facilitates co-existence with wirelessHART. ISA100.11a supports *Star* and *Mesh* network topologies.

WIA-PA. Wireless Networks for Industrial Automation - Process automation (WIA-PA) is an industrial standard proposed by the Chinese Industrial Wireless Alliance [12]. The aim was to design a high-reliability, energy efficient, and intelligent multi-hop WSN solution. It is fully compatible

with the IEEE 802.15.4 standard and is designed to provide a self-organizing and self-healing mesh network that is reactive to dynamic change in network conditions. The MAC layer is IEEE 802.15.4 compatible and a mixed CSMA, TDMA, and FDMA technology is used for medium access. It has 16 communication channels in the 2.4 GHz band and frequency hopping is supported. Three types of frequency hopping mechanisms are used: *Adaptive Frequency Switch*, *Adaptive Frequency Hopping*, and *Timeslot hopping* [66]. It supports inter-operability with legacy protocols like wired HART and various others like *Profibus*, *Modbus*, and also offers support for *wirelessHART*.

GINSENG. The GINSENG project [62], [67] aimed at developing a solution for performance control using WSN for time-critical applications. The idea was to present a deterministic MAC protocol that could meet the requirements of the application. The GinMAC protocol [68] is a TDMA-based protocol. GinMAC is a tree based protocol, whose development was envisioned to provide services like reliability and timely delivery of data for time-critical applications. The main techniques used in GinMAC are *Off-line Dimensioning*, *Exclusive TDMA*, and *Delay Conform Reliability Control*. GINSENG solutions are meant to be applicable for closed loop regulatory/supervisory systems and have been implemented in real systems to demonstrate its usability and performance [69].

Based on the summary of state-of-the-art wireless standards we discuss some recent advances and current market share. Among all these standards, wirelessHART and ISA100.11a are the two major and dominating standards already in the market. GINSENG is relatively new and it has not yet been widely deployed. In spite of the competition, the Hart Communication Foundation (HCF) and International Society of Automation (ISA) have agreed to collaborate together to produce one single standard derived from wirelessHART and ISA100.11a. A subcommittee named ISA100.12 has been created to investigate the possibilities of convergence [65], [70]. The convergence could result in a global standard with positives of both these standards and improved IWSN solutions. A comparison of the wireless standards (wirelessHART, ISA100.11a and WIA-PA) can be found in [66].

III. Security Function

Wireless networks are more susceptible to security attacks compared to wired networks, where the user will need to physically be connected to the network. For the same reason, the traditional wired security techniques do not satisfy the requirements of the wireless networks directly [71]. Important concept objectives are authenticity, integrity and confidentiality [72]. The importance on these factors depends on application specific requirements. The possible attacks on the wireless networks are node tampering, node control, denial of service, radio interference and other types of attacks [72]. It is a fundamental research challenge to implement security in WSN, considering the low cost of hardware used and energy efficiency being of high importance. For comprehensive information on security issues and solutions we refer to [73], [74], [75], [76]. In the current major industrial standards, security is an integral part of these standards and is treated with equal importance compared to other requirements. A dedicated security manager is used in wirelessHART, ISA100.11a and WIP-PA for security services [70]. Hence, security solution is an integral requirement of the WSN solutions, and below we discuss the solutions used in major wireless standards. In GINSENG, security is listed as an open issue and out of the scope of the project. This also affected its commercialization as a complete solution. [77].

WirelssHART. In wirelessHART, security is treated in both the MAC and the network layer. The MAC layer provides hop-by-hop data integrity using encryption mechanisms and the network layer provides end-to-end data integrity. The security manager application is implemented within the gateway device and handles all security services. The network manager is responsible for generation and storage of all keys required by the security services. Also, all security features in wirelessHART are mandatory unlike ISA100.11a [70].

ISA100.11a. Similar to wirelessHART, a security manager exists in ISA100.11a embedded with the system manager and gateway on the same physical device. The security manager in cooperation with the system manager is responsible for the generation, storage and distribution of the necessary security keys and is also supposed to manage authentication. The transport layer of the ISA100.11a node is responsible for end-to-end security [70]. The security feature is made optional in ISA100.11a to provide greater flexibility and improve battery life.

WIP-PA. WIP-PA also relies on a security manager to manage the security keys, authentication of field and other (gateway) devices [66]. On the nodes, the security services are treated on point-to-point basis on the data link layer and end-to-end on the application layer. Also, similar to ISA100.11a, security feature is made optional.

IV. Medium Access Control

Medium Access Control (MAC) protocols are responsible for controlling the medium access and deciding the underlying schedule for communication among the sensor nodes. The schedule should be designed according to certain application specific requirements. The scheduling problem can be solved using numerous methods which can be classified into three main classes [14] as described below.

Fixed Assignment Protocols. Available resources are divided appropriately among the sensor nodes and this division is applicable for a defined time duration. The resources are allocated to particular nodes and thus cannot be changed for the specified duration. The protocols in this class are based on medium access control mechanisms like Time Division Multiple Access (TDMA), Frequency Division Multiple Access (FDMA), and Code Division Multiple Access (CDMA). In TDMA-based MAC protocols, time is divided among the sensor nodes which requires time synchronization. In FDMA, the available frequency medium is divided into a number of sub-channels. 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. Fixed assignment protocols can be based on centralized control and distributed control. In the centralized control, typically the sink defines the schedule. In the distributed control, the scheduling control

TABLE I
COMPARISON OF TDMA AND CSMA PERFORMANCE

Condition	TDMA	CSMA
Delay on High traffic load	Controllable	High (Owing to collisions)
Reliability	High	Low
Predictable performance	Yes	No
Throughput considering increasing traffic	Increases	Decreases for high traffic

is divided among the nodes in the network. Certain chosen nodes define the schedule for the group of nodes they are responsible for.

Demand Assignment Protocols. Resources are provided to a node on demand. This allocation approach is limited to the duration required to communicate the data in hand. Once the data communication has been completed, the resources are returned. These protocols are adaptive towards change in network conditions and adjust their performance according to the traffic level. The protocols can be based on both centralized control and distributed control.

Random Access Protocols. This class of protocols is intended for distributed control. Certain advantages of randomness are exploited by dividing the resources randomly. Random access protocols are preferable for bursty traffic and dynamic changes in topology [14]. ALOHA [78] was one of the first random access protocols and is an important protocol in this class. In pure ALOHA, the nodes access the medium and transmit whenever they have data to communicate. Carrier Sense Multiple Access (CSMA) is a medium access mechanism which works on the principle of ALOHA, but the sensor nodes try to be more modest by sensing the channel when data has to be sent and send only if the channel is sensed free.

Hybrid Protocols. Recently, several protocols have been proposed that use fixed assignment protocols or demand assignment protocols in conjunction with random access protocols. These protocols combine CSMA and TDMA to exploit their advantages. One example is Z-MAC [79]. The combination of CSMA and TDMA can be done in several ways, one of them being TDMA slot scheduling at a higher level and allowing for contention within the scheduled slots. Another option is defining the schedule with a contention-free period and a contention period like in the Emergency Response-MAC [80].

In the following subsections, we discuss the importance of TDMA in IWSN and its advantages over CSMA. We then discuss some of the design considerations important for MAC protocols, but skip those design considerations which have already been discussed as a part of IWSN requirements. Then, we briefly discuss the classification of MAC protocols based on their goals and the requirements they satisfy. Finally, we survey some important representative protocols that partly or fully satisfy IWSN requirements.

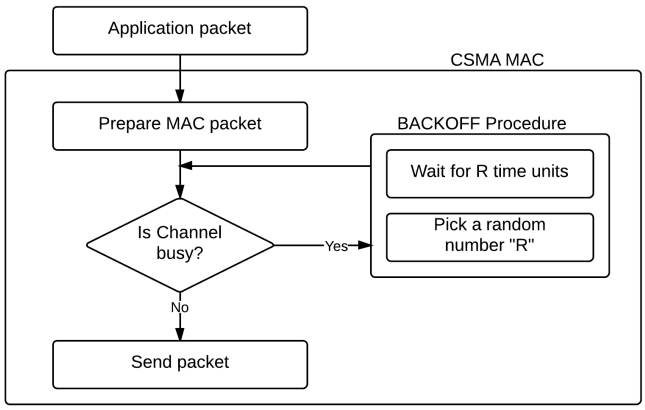

Fig. 4. Simple CSMA procedure

A. TDMA vs CSMA

The MAC function in most proposals for WSNs use either CSMA or TDMA. CSMA is contention-based and TDMA is reservation-based. The basic procedures for CSMA and TDMA are shown in figures 4 and 5, respectively. The studies performed by [81], [82], [83] show that TDMA-based protocols are more energy efficient than CSMA based on certain conditions of operation/scenarios. According to [84], [85] this is due to:

- CSMA methods suffer from significant collisions leading to retransmissions consuming more energy per unit of data.
- TDMA utilizes the bandwidth more efficiently under high loads thus resulting in higher energy efficiency.

Similar to the articles discussed above, comparison between CSMA and TDMA can be mostly given only based on the conditions of operation, since in some cases CSMA has an upper hand over TDMA. In this article, the main issues for industrial applications are reliability, predictability and delay sensitivity which can be addressed efficiently by TDMA schemes. TDMA with fixed slots is also more predictable than CSMA, which is a crucial element in selecting protocols for closed loop regulatory systems. TDMA has proved to achieve a high degree of reliability [86], since it is collision-free and predefined bandwidth allocation may be ensured. Although TDMA is energy efficient and collision-free, there are certain issues that require attention: synchronization [87] and efficient slot allocation [88]. Proper slot allocation techniques are required to ensure collision-free and interference-free channel access. TDMA also has issues in terms of scalability due to fixed time allocation and the requirement of time synchronization. In this context, we summarize the comparison between CSMA and TDMA in table I.

As an example to illustrate some performance differences between TDMA and CSMA we discuss a simulation study. Kulkarni et al. [83] simulated various scenarios and analyzed the performance differences between CSMA and TDMA-based mechanisms. The scenarios where: broadcast, convergecast, and local gossip. We particularly focus on the convergecast scenario (widely used by industrial networks) where the network setup was 10×10 grid with sensors in a subgrid sending messages to the base station at approximately the

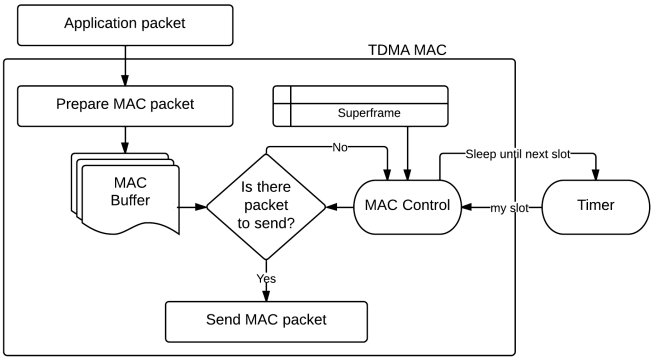

Fig. 5. Simple TDMA procedure with pre-defined slots represented by the superframe

same time. Significant collisions (10 to 15%) were observed in the CSMA based scenario with the increase in the number of nodes in the subgrid. The main observation was that in case of CSMA, 50% of the messages where lost due to collision with maximum 25 nodes sending messages simultaneously. Although TDMA suffered higher delay than CSMA mechanism it had a higher throughput given that all messages reached the base station successfully. Thus it severely affected reliability and throughput when CSMA was used. This description of comparison gives one instance of possibilities, the choice of TDMA and CSMA is more application dependent. In the industrial perspective, given the industrial requirements we focus more on the TDMA-based solutions in this article. Also, from the state-of-the-art industrial standards, we can observe that TDMA-based mechanisms are chosen mostly.

B. Design Considerations

Node Deployment. Different application scenarios have different topology for deployment of nodes according to their needs. The communication part has to consider this topology in order to effectively use the scarce resources of the nodes. The number of nodes deployed in a region also needs to be taken into account for efficient protocol design.

Control Packet Overhead. For various reasons like setting up of schedules, routes, and time synchronization, control communication is required. This is essential for the operation of the WSN. But this operation also consumes energy, bandwidth, and time, and thus may increase delay in communicating data packets. The MAC protocols should have limited overhead of control packets in order to be able to satisfy QoS requirements like low delay, high reliability, and high energy efficiency.

Time Synchronization. In the reservation-based schemes and hybrid schemes, it is important to ensure that the nodes are synchronized. The majority of functions and features in TDMA-based WSN work are based on time stamp, starting with slot reservation and communication. Thus efficient time synchronization [89] mechanisms have to be employed. Time synchronization can be further classified into two levels of synchronization: *local synchronization* and *global synchronization* [90]. In *local synchronization* the nodes in a region or a cluster (group of nodes) are synchronized while in *global synchronization* the entire network is synchronized. Thus implementation of synchronization is dependent on the protocol design.

Slot Scheduling. The process of slot allocation for medium access is known as slot scheduling. We have mainly chosen TDMA or reservation-based scheduling in the context of this article. Still, hybrid protocols that use CSMA along with TDMA may have advantages over protocols entirely based on TDMA. The standards like wirelessHART, ISA100.11a, and WIA-PA use hybrid scheduling for MAC. Thus it is an important design decision to choose from hybrid or TDMA-based protocols.

Duty-Cycling. This is a common mechanism in sensor nodes controlled by the MAC function, which defines the sleep period of nodes that are currently not involved in communication. By tuning the duty-cycle, the amount of energy used can be reduced. However, the duty cycle affects the latency. A low-duty cycle results in low energy usage but high latency. Thus there is a trade-off between latency and energy, and effective duty-cycling for an application would be one which maintains the required latency and also save energy.

Multi-Channel. Multi-channel communication is an effective method to reduce the effects of interference on the wireless medium by using different channels for communication and selecting the channel that has least interference. Recent sensor nodes support multi-channel communication and this has also been incorporated effectively into various industrial standards like wirelessHART and ISA100.11a. With multi-channels the possibility to communicate concurrently can also be exploited. It is a challenge to effectively perform channel switching while avoiding overlaps and maintaining coordination [91].

Cross-Layer Support. Moving further from traditional approaches of layered architecture and protocol solutions, researchers had proposed cross-layer implementation. These cross-layered proposals have also proved to be advantageous over the traditional approaches [92], [93]. By exploiting information from other layers, protocols can make more efficient decisions. The disadvantage of this approach is that by making different layers interdependent, the complexity of the protocol increases. This also makes the protocols hard to analyse. Another open issue here is to create generic APIs in protocols at different layers to support cross-layer communication.

Channel Utilization. Channel utilization is defined as the amount of bandwidth effectively used by the protocol for data transfer. With the use of TDMA-based protocols effective channel utilization can be achieved at higher data rates. For lower traffic, the MAC protocol has to function in such a way as to conserve energy when the application requires the sensor nodes to have minimal data transfer, e.g. temperature to be sensed and communicated every minute. Consider an application with heterogeneous nodes in a network, with common protocols implemented. The application requires temperature data to be sent every five seconds and pressure data to be sent every second. A TDMA approach may typically provide equal times slots to these node types and thus is not sometimes efficient. A CSMA approach could be more appropriate for such scenarios, or an intelligent TDMA slot scheduling that provides more slots for nodes transmitting more data. A hybrid

combination of TDMA and CSMA could result in effective channel utilization.

Node Priority. Service differentiation is provided at the MAC function by prioritization of different types of nodes. In hybrid protocols, nodes with higher priority get the channel access first for the CSMA part. In TDMA, higher priority nodes could be allotted more than one slot to facilitate reliable and higher data transfer. In clustering protocols, the cluster head (the leader of the group) has the highest priority and its participants have lower priority. Node prioritization is usually done statically, but it is also possible to change node priorities dynamically.

Collision Avoidance. With the use of hybrid protocols, the contention mechanism is partly used in the protocols. With the random access to the channel in contention based access, the possibility of collision is high. The occurrence of collision results in loss of packets, delaying of subsequent packets, increased retransmission, and decreased lifetime of the network. Thus collision has severe effects on the protocol performance. Effective measures have to be taken to prevent contention of nodes for the same slot, which are referred to as collision avoidance techniques.

C. MAC Protocols and Classification

MAC protocols [21], [22], [16], [23], [24] can also be classified according to their design goals. Previously, energy efficiency was the prime requirement [94] and best effort data delivery was sufficient. With time, design of MAC protocols has evolved [95] through different design goals, different techniques, and also different criteria have been used to classify the protocols. In the industrial context, energy efficiency has priority equal to requirements like reliability, low-delay, and robustness. Thus there is now a paradigm shift in design of MAC protocols towards protocols that satisfy these QoS requirements and also are energy efficient. Thus main classes of MAC protocols can be defined as *Energy-Efficient Protocols*, *QoS-Aware Protocols*, and *Real-Time Protocols*. *Energy-efficient Protocols* [96] have as their main objective to prolong network life-time and support as much data communication as possible within its life-time. There have also been studies of various energy saving mechanisms for MAC [97], and for WSN in general [98]. *QoS-Aware Protocols* aim at providing *application specific QoS* [49] and *network QoS* [99]. There has been a study of QoS-Aware protocols suitable for the WSAN scenario [100]. *Real-Time Protocols* [28], [29], [94] do fall in the class of QoS-Aware protocols, but are specified differently since they have now become a separate branch of research. These protocols are proposed for time-critical applications and they are especially useful for WSAN class of systems.

Below we shortly introduce some representative MAC protocols that are either proposed with industrial requirements or match crucial requirements for IWSN.

1) GinMAC: GinMAC [68] is a TDMA-based MAC protocol and has a tree topology. It was designed for time-critical data delivery. It was developed as a part of the GINSENG [62] project and is targeted on a specific application domain, in the form of an oil refinery. The main techniques used in GinMAC are *Off-line Dimensioning*, *Exclusive TDMA*, and *Delay Conform Reliability Control*. Low-duty cycling is used to save energy. GinMAC also has support for cross-layer communication. In the implementation of GinMAC the traffic patterns and channel characteristics are known apriori and all complex calculations including slot allocation is done off-line. Due to off-line dimensioning, the protocol has a more predictable performance. The maximum supported number of nodes is 25 and it is thus intended for small-scale networks. The allocated TDMA slots are exclusive in GinMAC and cannot be re-used by other nodes. Although these features restrict scalability of this protocol, it is not an issue since GinMAC is an application specific protocol used in the GINSENG [62] project.

2) QoS-MAC: The QoS-Aware MAC protocol proposed by Suriyachai et al. [101] aims at providing deterministic bounds for end-to-end delay and reliability. The design goals suit the requirements of the IWSN classes with QoS requirements. The authors have defined a collision-free TDMA-based scheme where the time axis is divided into a number of fixed-length slots called epochs. Cross-layer support is implemented by handling routing also at the MAC layer based on the topology awareness. A tree topology is assumed for node deployment. The protocol is supposed to ensure upper and lower bounds on end-to-end delay between nodes for convergecast network pattern. A retransmission scheme is also included in the cross-layer support and is employed to obtain improved transport reliability. It also employs certain techniques for energy efficiency using different duty cycling for different nodes depending on their position in the tree.

3) PEDAMACS - Power Efficient and Delay Aware MAC for Sensor Networks: PEDAMACS is a TDMA-based protocol and is mainly focused on achieving energy efficiency and delay guarantee simultaneously. It is designed for applications requiring periodic communication. It assumes a sink with uninterrupted power supply and with the ability to reach any node in the network with one single hop. The sink uses this ability to perform time synchronization, and the sink also performs tree topology discovery and slot scheduling. The nodes transmit data to the sink via intermediate hops. PEDAMACS attempts to eliminate network congestion and provides end-to-end bounded delay guarantee. The traffic data is generated at each node and is transmitted to the sink which takes appropriate measures to manage the traffic.

4) ER-MAC - Emergency Response MAC: Lanny et al. [102] proposed ER-MAC to serve applications requiring emergency response. It is a hybrid (TDMA and CSMA) MAC protocol designed with the main goal of providing high level adaptivity [80]. ER-MAC provides both traffic adaptability and topology adaptability, and thus is also scalable as per the proposal. It initially communicates using CSMA with collision avoidance (CSMA/CA), creates a data gathering tree and assigns TDMA schedules. It divides the frame into contention-free slots and a contention period. The contention period is used to support the addition of new nodes. For energy conservation, nodes that do not have any data to send on their assigned slot do not switch on their radio. ER-MAC implements different modes, normal mode for normal operation and emergency mode to facilitate emergency response. Nodes in emergency mode have the highest priority. Local

time synchronization is used, by exploiting the tree structure such that each child synchronizes with the time of its parent.

V. Routing Function

IWSN consists of a network of nodes and data is communicated between two nodes e.g. between a source and a sink. These are usually multi-hop networks where each sensor node needs to send data. Thus we have multiple nodes attempting to send data via intermediate nodes creating traffic that requires efficient management to satisfy the IWSN QoS requirements. Routing protocols are used for efficient routing of the data through the network. Over the years, various routing protocols have been proposed [26], [18], [25] to satisfy the QoS requirements. We discuss the most relevant protocols and also the main design requirements for an efficient routing protocol. There are many design requirements [18], [25] that can be used to select a routing protocol. We focus on requirements relevant to the IWSN classes of systems as defined in this article. Detailed information on various routing metrics e.g., average path length, that have to be considered during design of routing protocols has been provided by Khan et.al. [103] and for industrial routing requirements in [104]. The routing metrics have two use cases; firstly they can be used to evaluate a proposed routing protocol by describing the performance in terms of the metrics, secondly the routing metrics are used by the routing protocols to construct efficient routes [105] dynamically. The requirements also partly include network layer functionalities implemented to forward packets that affect the routing decisions made. Packet scheduling and packet priority are two requirements involved in the packet forwarding process.

A. Design Requirements

Fault Tolerance. IWSN nodes dominantly run on batteries and hence node failure is likely. There could also be other causes of failure of sensor nodes. These failures affect network connectivity, especially when intermediate nodes fail, several nodes are affected. Routing protocols are responsible for handling these failures by both identifying these failures and creating an alternative path around the failed node. An alternative solution is that the routing protocols have multiple paths enlisted for each destination node in the network. This alternative path creation can be time-driven or response-driven. Time-driven protocols are the ones where the links are checked periodically and new alternative paths created in case link failure is detected. Response-driven protocols are responsive to change in network dynamics such as failure of certain links and increase in traffic. New alternate paths are created in such cases.

Energy Efficiency. One of the most important requirements of WSN and also IWSN is energy efficiency considering the limited capacity of batteries. In a multi-hop network, sensor nodes have two functions: sending data and forwarding data. Routing protocols need to consider methods to reduce energy consumption by creating data forwarding paths that are energy efficient.

Load Balancing. Along with energy efficiency, load balancing is important in order to increase the overall network lifetime. Intermediate nodes near to sink in large networks have high traffic load resulting in early depletion of the battery and node failure. This results in increased delay and loss of data packets and furthermore node failure makes it difficult for the routing protocol to maintain network connectivity. Thus efficient load balancing techniques have to be employed in order to increase the network lifetime, decrease delay, and increase throughput.

Data Frequency. Applications have different data reporting frequency depending on the requirements. Common possibilities are:

- *Time-driven*: Sensor nodes collect data continuously and send them in a periodic manner. The size of the data packets and time frequency are decided apriori and thus is predictable.
- *Event-driven*: Data is measured and collected continuously but sent only when the data measured represents previously specified importance, e.g., an event. The time of occurrence of an event is unpredictable.
- *Query-driven*: Continuous collection of data where sending is initiated only when the sink sends a query to the respective sensor node. Similar to the event driven scenario, the occurrence of a query is unpredictable.

This frequency of sending data has an impact on the performance of the routing protocol and hence has to be considered prior to designing the protocol.

Packet Scheduling. The routing function also determines how the packets are forwarded at the intermediate nodes between a source and a destination. Before the packets are forwarded, each incoming packet is put into a queue. This insertion happens according to a scheduling algorithm, e.g. first in first out. Various alternative packet scheduling algorithms could be implemented for this purpose. The packet scheduling is also affected by the *packet priority*.

Packet Priority. In routing, *service differentiation* is done at the packet level. A packet can be marked with different priority levels. At the intermediate node where the packet scheduling is done, the packets are treated according to their priority. Although this decreases the delay in delivery of the higher priority packets, it increases the overhead of the routing protocols.

Packet Aggregation. In the routing function, similar to data aggregation at the application layer, packet aggregation can be performed. In a network the maximum packet size is set to a certain constant but actual packet size depends on the data generated and can vary for each sensor. At the intermediate node, two or more packets destined to a single destination can be combined given the combination of packets is still equal to or lesser than the maximum limit. In *convergecast* communication, the sink is the only destination in the network. But, for some applications there could be multiple destination nodes, especially in the case of WSAN.

Node/link Heterogeneity. Most IWSN have homogenous sensor nodes, but particularly WSAN have heterogeneous nodes. Thus WSAN requires special routing protocols which considers this difference between the type of nodes i.e., sensors and actors. These two types of nodes are different in terms of resources and capabilities. Also, different types of nodes require different kind of communication, e.g. the

communication pattern between two sensors, sensors-actors and two actuators will often be different.

Expected Transmission Count (ETX). Considering the high probability of link loss, the routing protocols are also assessed by the expected transmission count. This metric describes the maximum number of transmissions required per packet to reach the neighbor with the available link conditions.

B. Routing Techniques

Routing protocols can be classified based on network structure, functions provided, QoS provided and other operational requirements [18], [25]. We discuss the classes of routing techniques relevant to the IWSN classes of systems defined. First, we consider techniques based on network structure.

Flat routing. In this approach all nodes have equal capabilities and functionalities. Data-centric query driven routing protocols are listed in this class. This technique is suitable for applications requiring a large number of sensor nodes and where nodes placed in a small region record same or similar data. The base station sends in a query to a region of interest and depending on the data request the nodes reply via data packets. Important protocols in this class are *Sequential Assignment Routing* (SAR) [106] and Directed diffusion [107]. Based on these protocols numerous protocols have been proposed over the years. Important characteristic of flat based routing is that it has mostly contention based MAC.

Hierarchical routing. The sensor nodes are divided into clusters/groups and each of these clusters are managed by a sensor node known as a cluster head (CH) with special functions which lies at a higher level of the hierarchy in the network than its peers. An example scenario of clustering is shown in figure 6. There are various algorithms to decide on the clustering of nodes and selecting CHs [108]. Although, the hierarchical routing techniques are usually TDMA-based and according to Al-Karaki et al. [18] is more energy efficient than flat-based routing, the results are size dependent. Major routing techniques in hierarchical routing are LEACH [109], HEED [110], and TEEN [111]. Based on these protocols various new protocols have been proposed [112], [113]. The initial proposals of hierarchical routing protocols are based on a specific architecture, with nodes at a distance of one-hop from the CH and the CH is one-hop distant from the sink. In recent years, multi hop hierarchical protocols like ARPEES [114], *Asymmetric multi-hop communication* [115] and also multipath protocols like MuMHR [116] have been introduced which aims at providing scalability by multi-hop and reliability via multiple paths.

Location-based routing. In *location-based* routing, the location of the sensor nodes are known and is exploited in making routing decisions. The sensor nodes are equipped with Global Positioning System (GPS) or other localization facilities to determine their position and relay it to the base station. For IWSN, we assume that sensor nodes are static and do not require GPS and thus location can be calculated during installation.

Routing protocols can also be classified based on the protocol operation and type of service they aim to provide. QoS service is one of the main aspects provided by routing protocols and is a broad classification. It can be further classified into various classes, but in this article we focus on the QoS requirements of IWSN.

QoS based routing. QoS based routing techniques aim at satisfying particular QoS requirements. Main QoS requirements are reliability and real-time guarantee for the first four classes of industrial systems (section II). Sequential assignment routing (SAR) listed in flat routing can also be listed here and it is one of the important protocols in QoS based routing protocols along with SPEED [117] and MMSPEED [118]. Recently, this area has developed into a dedicated branch of research [94], considering the industrial requirement of timeliness in routing especially for WSAN.

Multipath routing. Multipath routing aims at creating redundant paths to route data packets to facilitate reliable and timely delivery of data to the sink. It also ensures load-balancing and fault tolerance [119] satisfying important design requirements. Multipath routing also aims at satisfying QoS, but can be classified separately considering the huge number of protocols proposed in this domain. MMSPEED, SPIN [120], and Directed Diffusion based *Highly resilient, energy efficient multipath routing protocol* [121], are some of the important routing protocols that use multipath routing. Multipath routing protocols can be further classified as *disjoint multipath* and *braided multipath*. In *disjoint multipath*, the alternate paths created are node/link disjoint with the primary path. In *braided multipath*, a set of alternative paths are created in which each alternate path is created for a node in the primary path by skipping that node.

Fault tolerant routing. Fault tolerance is one of the IWSN requirements and is critical for some classes of systems for proper operation. Fault tolerant routing protocols thrive to provide robust routing mechanisms that are less affected by failure of nodes and links. Fault tolerant routing increases the reliability of the system. These routing protocols can be further classified into *retransmission* based and *replication* based [122]. *Highly resilient, energy efficient multipath routing protocol* [121], REAR [123], and ReInFoM [48] are some of the protocols in this class which are based on the Directed diffusion protocol [107].

C. Routing Protocols

In this section, we discuss some candidate routing protocols capable of addressing some of the requirements of considered industrial classes. Two relevant routing protocols designed for WSNs are RPL [124] and MMSPEED [118], two other protocols are hierarchical protocols HEED and TEEN, which other than defining the routing function also defines the medium access. Below we discuss these protocols briefly.

1) RPL - Routing Protocol over Low-power and Lossy Networks: RPL [124] is a protocol designed by the IETF working group ROLL. It is an IPv6 based gradient routing protocol. It is proposed for convergecast network structure in WSN which is also the network structure of the major industrial standards wirelessHART and ISA100.11a. The main goal of RPL is to construct efficient routing paths for the network. It was designed to supports three traffic patterns: multipoint to point (source to sink), point to multipoint (sink

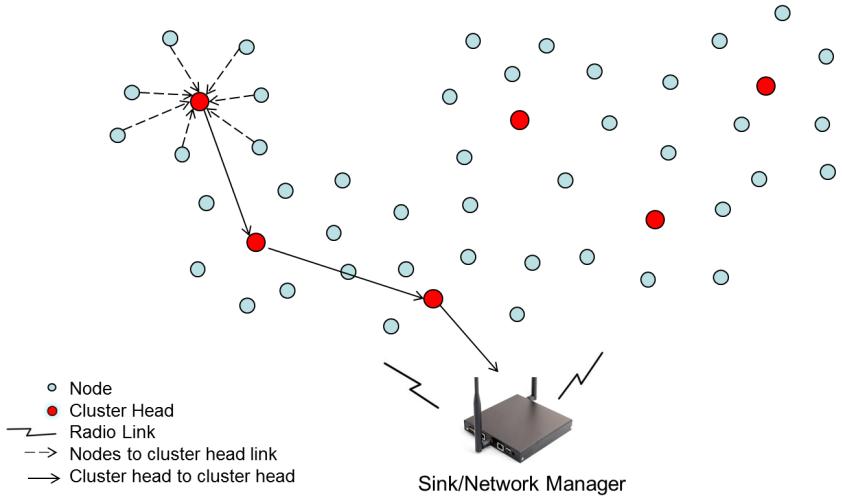

Fig. 6. An example scenario displaying clustering

to source) and point to point (source to source). In RPL, based on the sink, a tree like routing structure is created by allowing each source node to send data packets to the sink with minimal cost, where node information is used in this construction. The link cost and node information also includes other routing metrics [105], e.g., residual energy, throughput, latency. RPL is a proactive protocol and hence dynamically changes with change in traffic. The tree like structure used by RPL is called a Destination Oriented Directed Acyclic Graph (DODAG). To be applicable to various applications, RPL isolates routing optimization techniques from packet processing and forwarding. With the use of IPv6, RPL opens up the possibility to connect to the Internet. Performance analysis [125] of this protocol has also been done by the designers to conform that the protocol adheres to its specifications and assess the control overhead. Similar performance analysis studies have been performed by external sources assessing the efficiency of the protocol including overhead, identifying problems and providing suggestions for improvements [126], [127], [128].

2) HEED - A Hybrid, Energy-Efficient, Distributed Clustering Approach for Ad Hoc Sensor Networks: HEED [110] is a hierarchical protocol proposed as an energy efficient solution for WSN with the aim to maximize network lifetime. HEED has the basic assumption that sensor nodes have multiple transmission power levels, which is not always true. It has a hybrid approach in terms of CH selection, which considers both residual energy and communication cost. Sensor nodes with high residual energy are eligible to become CHs. Along with this hybrid approach, HEED also consists of three main characteristics (according to [110]): the probability of CHs being well distributed in the network is high; energy consumption is assumed to be uniform; probability of CH selection can be adjusted to ensure better inter-CH connectivity. The authors have also mentioned features like scalability and fault tolerance along with its primary goals.

3) TEEN - Threshold Sensitive Energy Efficient sensor Network protocol: TEEN is a hierarchical protocol proposed as a protocol for time-critical applications. It is an event-driven protocol aimed at event-based applications. Once the clusters are created and a CH has been selected, the CH broadcasts two thresholds to its cluster nodes. The two thresholds are related to the value of the data and are referred to as soft threshold and hard threshold. When the sensed data of a node exceeds the soft threshold, the data is sent to the CH which relays it to the sink. When the hard threshold is exceeded the sensor node directly relays the data to the sink. The CHs are changed periodically for load balancing. TEEN is event-driven and hence periodic data collection was not designed in the protocol. Thus, a hybrid model which is suitable for both periodic data-collections and time-critical events was proposed, the protocol was named Adaptive TEEN (APTEEN) [129]. In APTEEN, in addition to the basic functionalities of TEEN, additional parameters are defined that a user can query on, e.g. a *count time* which is configurable by the user. When no threshold has been reached for the duration of count time, the sensors are forced to send any sensed data thus creating the notion of periodic collection. Due to the introduction of these new features the complexity of the protocol is higher than in TEEN. *Power-efficient & Increased Yield Approach* (PRIYA) [130] was proposed to overcome this overhead by creating two CH's instead of one. One CH is used for data aggregation (DCH) and the other CH is used for routing (RCH). The changing of CH was based on energy spent of the CH and not done periodically like in TEEN or APTEEN. Unlike TEEN and APTEEN, PRIYA does not set thresholds but defines a range of data which when sensed has to be communicated to the base station. PRIYA was compared with TEEN, APTEEN, and LEACH, and was found to be more efficient than its counterparts until the nodes starts dying due to energy depletion, after which the performance deteriorates rapidly [130]. It is also worthwhile noting that TEEN does not only propose routing functionalities but also medium access control and requires application layer data to be compared to the threshold measured.

4) MMSPEED - Multipath Multi-SPEED protocol: MMSPEED [118] by Felemban et al. was proposed as an improvement over SPEED. The aim of MMSPEED is to provide probabilistic QoS guarantees and service differentiation. MM-

SPEED facilitates timeliness by providing multiple network-wide packet delivery options depending on the traffic type and their end-to-end deadlines. The protocol relies on probabilistic multipath forwarding. Similar to SPEED, MMSPEED does not have global network state information and works locally to set up paths. It is thus scalable and reactive to dynamic changes in the network. MMSPEED focuses entirely on QoS services and are meant for applications which do not focus on energy conservation.

VI. Transport Function

Reliability is an important requirement of industrial systems. Transport protocols for WSNs are responsible for improving reliability and for congestion avoidance. To ensure reliable data delivery, the WSN should be able to detect packet loss and enable the retransmission of lost packets. Congestion control is commonly done either by dropping packets or by delaying the sending of packets, thus decreasing the number of packets in the network. Alternatively, it is also done by setting the congestion notification bit which is sent as a control message, this is known as Explicit Congestion Notification (ECN). In recent years, several transport protocols have been proposed for WSN. Some of these protocols focus on either reliability or congestion control and others address both features.

We firstly discuss the various features for the transport protocols and the best suited design options considering the framework of wirelessHART, ISA100.11a, and GINSENG, starting with the reliability and then covering congestion. We conclude this section by discussing some important transport protocols proposed for WSN and applicable to IWSN.

A. Reliability

Considering the general design scenario of IWSN with multiple sources and a single sink, reliability can be established in two directions: firstly for the control packets sent from the sink to the source and secondly the data packets sent from the source to the sink. These reliability directions provided by the transport protocols are *upstream reliability* and *downstream reliability*.

- *Upstream reliability*: Upstream reliability is essential to ensure successful delivery of packets from source to sink. Given the convergecast nature of wirelessHART, the control packets go from sink to nodes and the data packets go from source to sink. Hence, an ideal transport protocol should have reliability direction of at least upstream reliability or both (downstream reliability is discussed below). Most of the proposed transport protocols [131], [132], [133] provide upstream reliability.
- *Downstream reliability*: Downstream reliability ensures the reliable transfer of query and control packets from the sink to the source (nodes). In the view of low-power lossy networks with unreliable links, the downstream reliability is important in most of the industrial cases. The protocol ART [132] provides bidirectional reliability i.e, both upstream and downstream, and could be an important protocol for systems requiring high reliability.

Reliability Level. The reliability level defines the classification made by transport protocols to decide the importance of packets. There are mainly three reliability levels:

- *Packet level*: In packet level reliability, every packet has equal priority and the delivery of every packet has to be ensured. This is particularly important for certain applications that require continuous delivery of data with high reliability.
- *Event level*: In event level reliability, particular events are identified apriori and the packets that contain information about the event have higher priority than other packets.
- *Node level*: In node level reliability, every node is given a priority index and the packets being forwarded are checked for priority and packets from lower priority nodes are dropped first in case of congestion.

The selection of the type of reliability level also depends on the QoS requirement of the application. Selecting the packet level reliability results in more energy consumption than the event level since each packet has to be accounted for. For event level reliability, the sensor nodes have to be pre-configured with the list of events that have prime importance. Similarly, nodes are required to be pre-configured with node level priority. Dynamic prioritization is also possible but requires complex algorithms and high processing power which is absent in low-power sensor devices. The reliability level required in the industrial systems is different for different classes depending on the QoS requirement of each class.

Loss Detection. For retransmission of packets, the packet loss has to be detected. The loss detection can be either at the *sender* side or the receiver side. At the sender side, the loss detection is done with the use of a timer. The timer is set to the maximum anticipated time required for the round trip, starting from the packet being sent until the acknowledgement for that packet is received. This is known as the round trip time (RTT). At the receiver side, the loss is observed when out of sequence packets arrive.

Loss Notification. In traditional wired networks each packet has a unique sequence number and using this sequence number, the receiver sends an acknowledgement packet to notify the sender about packet reception. When the sender does not receive this notification within a certain time, it retransmits the packet assuming loss of packet. Transport protocols designed for WSN have similar feedback techniques. Three basic types of feedbacks exist:

- *Positive acknowledgements* (ACK): The acknowledgements sent for the received packets are referred to as ACK. These acknowledgements are sent as control packets, which could be either implicit (iACK) or explicit (eACK). For eACK, the receiver explicitly sends acknowledgements. In iACK, nodes overhear packets being forwarded and if so then the sender silently deletes the packet from its buffer.
- *Negative acknowledgement* (NACK): In a stream of packets received, the missing packets are identified by the receiver and the sequence number of these packets are sent to the sender. This type of feedback mechanism is called negative acknowledgement. NACK can either be sent for a single packet or for a range of packets.

- *Selective acknowledgements* (SACK): In SACK for a segment of data, the last received fragment is acknowledged and the sender has to send the rest of the fragments. SACK aims to reduce the energy consumption and congestion by reduction of control packets, but this can be disadvantageous in some scenarios. One particular scenario where n fragments make a segment and even when only the $(\frac{n}{2}+1)$th fragment is missed, half the number of fragments have to be sent again. In this scenario the energy consumption is above the average energy consumption.

Loss Recovery. In transport protocols, reliability is provided by detecting lost packets and re-transmitting them. This procedure is called loss recovery and can be done in two ways:

- *End to end*: Similar to the traditional wired network methods, the end points are responsible for loss detection and recovery.
- *Hop by hop*: In the hop-by-hop approach, packets are cached at each hop and are deleted only after the delivery of the packet to the next hop node is successful. Note that the link layer also employs a hop-by-hop approach which differs from the one in the transport layer, because this approach is carried out for each packet sent. With the hop-by-hop method as a part of the transport function, once the source delivers the packet to its next hop successfully, it deletes the packet from its cache and the next hop is entirely responsible for the packet reaching its destination.

Both methods have their own advantages. Using end-to-end we eliminate the overhead of caching packets at each hop. The hop-by-hop method is scalable because with the increase in number of hops, the requirement to re-transmit data end-to-end can induce considerable amount of delay in the network. The hop-by-hop method is considered to be more suitable for WSNs than the end-to-end method [19], [134], [135]. Considering the lossy nature of the links in the low-power WSNs, the possibility of a packet to be lost is higher than in wired networks. When the end-to-end retransmission is used in multi hop networks, each lost packet requires a control packet to be sent back to the sender. Next the sender has to re-transmit the packet or has to wait until its retransmission timer goes off. This causes an increase in the overall energy consumption of the network with high link loss probability. The above mentioned issues have also been confirmed by [136], [137] which demonstrates that the hop-by-hop approach is more scalable and error tolerant than the end-to-end method. The hop-by-hop method on the other hand introduces a security vulnerability of the transport function allowing the processing of the transport header at intermediate nodes [138]. This topic is further discussed in section VII.

B. Congestion

Congestion in WSN, can be caused by different reasons and is more likely to occur at the nodes near to the sink in centralized systems and at the cluster heads for de-centralized systems. It can be caused by an increase in packet arrival rate beyond the node's transmitting rate. It can also be caused by increased retransmission of packets due to packet loss. The direct implications of congestion are: an increase in average delay of the network, excessive packet drops and re-transmissions. Thus congestion control is important in WSN, especially in delay sensitive networks. Three important functions are used to control congestion: *congestion detection*, *congestion notification* and *congestion avoidance*.

Congestion Detection. Congestion detection can be done via one of the three approaches. Firstly at the sender side using a timeout for each packet, secondly by the sender via receipt of redundant acknowledgement (this happens mostly in the end-to-end scenario) and lastly at the intermediate nodes when the packet processing is slower than packet arrival rate. Different protocols use different methods to detect congestion and can use various parameters listed in [19], [27].

Congestion Notification. Congestion notification applies to the last method of congestion detection where intermediate node detects the congestion. The node needs to notify either the sink to take appropriate measure or the sources that are responsible for the congestion or inform all the nodes in the network. In a centralized system, most protocols use the sink to take appropriate measures to control the congestion. The congestion notification can be done either via bits called a congestion notification or a more detailed control packet with additional information about the congestion. Similar to loss notification, we have *implicit* and *explicit* congestion notification or ECN, where implicit relies on overhearing and ECN is sent as control message.

Congestion Mitigation/Avoidance. Once the congestion is detected in the network, we need to mitigate it in order to prevent the increase of delay in the network. Transport protocols implement various functions to make this possible, some of which even try to avoid the possibility of congestion by regulating the production of packets at each node. The common methods to mitigate congestion are:

- *Rate adjustment*: Rate adjustment is done at the source node when they receive a congestion notification. The control decisions for the rate adjustment depends on the network architecture. In a centralized system, the sink is responsible for this and in a decentralized system, the CHs or each node decide on the rate adjustment.
- *Traffic redirection*: When the congestion occurs at particular nodes, alternate paths with less or no congestion are used to forward the packets. Congested paths are noted and are avoided.

C. Transport protocols

Below, we discuss some representative protocols that satisfy transport requirements for the considered classes of systems. The three protocols discussed here are ART, RT^2 and RBC, each designed with different goals in mind.

1) ART - An Asymmetric and Reliable Transport Mechanism for Wireless Sensor Networks: Nurcan and Wenye introduced ART in 2007 and it aims at providing event and query reliability in addition to other features like scalability and energy efficiency. Being bi-directional, it succeeds at providing a high level of reliability. For scalability, ART provides reliability only to a subset of the sensors and this subset changes with time to ensure energy efficiency. It uses

an energy efficient classification of sensors into essential nodes and normal nodes. The essential nodes are provided with transport services for reliability both for event and queries. The query reliability and event reliability are treated differently. For queries, a NACK mechanism is used for notifying the sink whenever the loss of a query occurs. This loss is essentially discovered using the sequence numbers of the query messages. In case of event reliability, an ACK mechanism is used since events could be obtained from any node and sequence numbers were not implemented. This ACK is sent only for event alarm messages which are explicitly notified by the sensor to the sink. In both cases, end-to-end reliability is implemented at both the sender and receiver side, making both sides responsible for loss detection in query reliability and the sender being responsible for event reliability via retransmission timers. Distributed congestion control is used for better energy efficiency. The essential nodes detect congestion by using a timer for the event alarm messages. If the ACK is not received in time, the traffic from non-essential nodes is reduced by sending congestion alarm messages, which is repeatedly sent until congestion is relieved.

2) RT^2 *- A Real-Time and Reliable Transport Protocol for Wireless Sensor and Actor Networks:* Gungor et.al. [131] proposed a transport protocol for Wireless Sensor Actor (e.g. Actuator) Networks. The main goal of RT^2 is to improve reliability and congestion control with minimum energy consumption in heterogeneous networks. RT^2 aims at providing reliable services satisfying application specific real-time delay bounds. The sensor-actor and actor-actor communications are treated with different reliability requirements. They assume the communication between sensors and actors to be not as important as communication between actors. Thus the reliability level between sensor-actor communications is set to be event level and between actors, packet level reliability is used. Reliability is only provided upstream. RT^2 also employs congestion detection and congestion avoidance mechanisms. Congestion detection is based on average node delay and buffer occupancy. Rate adjustment is used for congestion avoidance and congestion mitigation. They address five different combinations of reliability and congestion in the network with appropriate measures for each combination. RT^2 was originally designed for CSMA based MAC and a case study with CSMA/CA based MAC protocol is presented. The protocol can be modified to TDMA. The only CSMA based concept is in the time to deadline calculation which can be ignored since TDMA needs a global synchronization clock.

3) RBC - Reliable Bursty Convergecast: RBC for WSN was proposed by Zhang et.al. [133]. The primary purpose of this protocol is to satisfy reliability requirements of real-time applications. RBC uses window-less block acknowledgements for improved channel utilization. Block acknowledgements also decrease the probability of ACK loss by replicating the ACK for a received packet. RBC was proposed for CSMA based MAC implementations and hence attempts to reduce contention by ranking the nodes according to various parameters. The reliability direction is upstream and is provided end-to-end. At the MAC layer, RBC employs hop-by-hop retransmission for better reliability. Adaptive retransmission timers which vary based on the network state are used to compensate for the continuously varying ACK delay. Although adaptive retransmission timers enhance the performance, it is still based on conservative calculations. To reduce the delay due to conservative measurements, RBC uses block-NACK, channel utilization protection (CSMA based) and retransmission timer reset.

VII. Research Challenges and Future Directions

With the advances in IWSN research, various industrial standards have been proposed. There are also ongoing attempts to merge the two major standards wirelessHART and ISA100.11a to benefit from the advantages of both. In addition, various protocols, frameworks, and techniques have been proposed to improve state-of-the-art. However, this has in turn posed new challenges. Discussion of challenges on IWSN and WSAN can be found in some studies [30], [9] and [139]. Most of these challenges have been presented and discussed already in the requirements section of this article. In this section, we focus on co-existence and coordination issues, which are two of the challenges present in literature which are still unresolved. We also discuss some new challenges and future directions that we consider important from the IWSN perspective.

A. Single Point of Failure

WirelessHART has a centralized control implemented in the form of a Network Manager. The downside of having the centralized control is that it could result in being a single point of failure and also a bottleneck in case of high traffic. Also, failure of nodes in the vicinity of the network manager may result in routing problems for the network manager causing packet loss and routing loops.

B. Scalability

Scalability is an important issue in the wireless standards mentioned, mainly in industrial standards like wirelessHART and ISA100.11a. These standards are dominantly TDMA-based. The need for synchronization and the time duration of slots in combination with QoS requirements, limits the number of nodes that can be included in a network. Furthermore, these standards are centralized, which limits the scalability. Given the numerous applications in the industrial domain, each application could have different requirements in terms of number of nodes. Solutions like wirelessHART do not scale to large number of nodes, thus designing solutions that can scale to operate with a large number of nodes is a challenge.

C. Hop-by-Hop vs End-to-end

The hop-by-hop retransmission method used in the transport function is preferred over the end-to-end method for WSN in several approaches [19], [134], [135]. The important reasons for this is that with high probability of link loss, the scalability of hop-by-hop is better than end-to-end. When the number of hops increases, the retransmission is costly in terms of resources in end-to-end solutions. End-to-end potentially generates too much traffic as packets must be re-transmitted along the path, but it can forward along an alternative path thus

preventing jitter and congestion. Hop-by-hop has its downside as well, as the high probability of link loss could also result in recurrent transmissions and the overhead to read the packet headers at each hop. Hop-by-hop could also result in waste of considerable amount of resources when the destination node is dead. It can also be possible that the next hop node is dead and the data packet can never reach certain destinations due to this. Alternatively, we could suggest that IWSN with a node downtime of few minutes could benefit from hop-by-hop approach, while IWSN with node downtime for a few hours or days could benefit from the end-to-end approach.

D. Co-existence

Designing low-power wireless networks for IWSN to co-exist with other wireless standards is a design requirement. There have been attempts to address this essentially by channel blacklisting and frequency hopping as in wirelessHART [13] and it has also resulted in improving co-existence [140]. Yet collisions happen and also affect the QoS of the protocols and standards. Thus more effective mechanisms to resolve co-existence issues are required.

E. Predictability

Predictability is one of the main IWSN requirements. An IWSN in itself is quite complex with various layers with different functionalities implemented. The non-determinism and unpredictability in some of these functions renders the communication part unpredictable. It is a challenge to create network protocols that satisfy the desired requirements in addition to supporting predictability. For instance, the use of event-driven data frequency pattern induces unpredictability in the routing function. Thus there is a need to build protocols that are predictable in addition to the functions and services they provide.

F. Multiple Source Multiple Sinks

Although this is not entirely a new concept, the work done in this area is minimal. The routing solutions [141] for multiple sources to multiple sinks are particularly important in WSAN. WSAN can also have a centralized setting where the network manager decides the schedules and handles time synchronization, and where the sinks in this case are the actuators. Thus there is a need for protocols that cater for the need of different data packets with different priorities to be routed using the same network, in order to meet the QoS requirement for each packet.

G. Lack of Protocols for WSAN

To the best of our knowledge there have been minimal proposals for MAC protocols for WSAN in comparison to general WSN proposals. With special requirements of WSAN like time boundedness, robustness, and service differentiation, MAC protocols dedicated to satisfy these requirements are needed. Especially to provide different implementations for sensor nodes and for actuator nodes, since both are different in terms of resource availability. This heterogeneity imposes new challenges for the design of protocols by increasing the design complexity. Similarly, work on routing and transport protocols for WSAN is minimal. This class of industrial systems is fast growing and highly demanding, thus protocols have to be developed to satisfy WSAN requirements.

H. Coordination

Coordination among actuators is required to take cooperative decisions on certain actions. In order to make appropriate decision, actuators need to communicate among themselves, thus communication is an important part in coordination. The method in which the coordination is carried out depends on the network architecture. It could be centrally controlled where the network manger decides on the actions and instructs the actuators to take action. Alternatively the control could be performed in a distributed architecture. Various protocol proposals have been made in this regard. For further details [9], [142].

VIII. Summary and Conclusion

In this article, we have surveyed and discussed systems and protocol candidates for medium access control, routing and transport functions in IWSN. The assessment was based on the presented classification of IWSN and in accordance to its requirements. Below, we summarize the classes and discuss the candidate protocols that could be used in the network solution for these classes. This is also summarized in the table II and discussed further below.

1) Safety system: Safety systems require emergency action, thus prime requirements are time bounded delivery, reliability, and availability. ER-MAC is a custom built MAC for emergency response and hence is also suitable for safety systems. A good solution for routing could be a QoS based multipath routing protocol like MMSPEED which focuses on timely delivery. The requirement on energy efficiency can be lowered due to trade-off to obtain better reliability. For the transport function, a protocol with the good features of both RT^2 and ART would be a good choice. Protocols should be event-based both for the transport and routing functions. RBC could also be a choice considering that it has real-time and reliability features.

2) Closed loop regulatory system: Closed loop regulatory systems require timely data and action with requirements like timely delivery, reliability, availability, and energy efficiency. GinMAC is appropriate due its features, but it is limited in terms of scalability since it is designed for maximum of 25 nodes. On the routing part, protocols like RPL, which was proposed based on the industrial requirements is appropriate. Since the requirement is continuous delivery of data, a stable routing protocol which has reliable and timely services with minimum to no failure is important. Energy needs to be considered here unlike safety systems since untimely death of nodes could disrupt the network connections resulting in degraded service. Timeliness and reliability are the most important requirements. RT^2 is a real-time protocol proposed for WSAN and is appropriate for the transport function.

TABLE II
SUMMARY OF CLASSES AND PROTOCOLS.

Classes	**Prime Requirements**	**Protocols**		
		MAC	Routing	Transport
Safety System	Time-bounded delivery, reliability, and availability	ER-MAC	MMSPEED	Combination of RT^2 and ART
Closed Loop Regulatory System	Time-bounded delivery, reliability, availability and energy efficiency	GinMAC	RPL	RT^2/RBC
Closed Loop Supervisory System	Reliability and energy efficiency	PEDAMACS, QoS-MAC	RPL	ART
Open Loop Supervisory System	Reliability and energy efficiency	PEDAMACS, QoS-MAC	TEEN/APTEEN	ART
Alerting System	Reliability, availability and energy efficiency	ER-MAC with more focus to energy efficiency	TEEN/APTEEN	ART
Monitoring System	Energy efficiency	HEED (clustering)	HEED	Not Required

3) Closed loop supervisory systems: The prime requirements of closed loop supervisory systems are the same as that of closed loop regulatory systems, but since sensed data is required only in supervisory control, the importance of reliability, availability and timely delivery is relatively less critical. Thus MAC protocols giving equal importance to time bounded delivery and energy efficiency like PEDAMACS and QoS-MAC are suitable. Routing protocols similar to closed loop regulatory system can be used here, e.g., RPL. For the transport function, end-to-end approach could be more appropriate since data requirement is not continuous which means that less data has to be catered for. Hence, ART could be a good solution.

4) Open loop human control: With the human in the control loop, the time-criticality of the data communicated by the nodes is far less. Event-based, energy efficient, and decentralized clustering protocols like TEEN/APTEEN would be appropriate in this case. TEEN/APTEEN also decides the strategy for routing and is hence a solution for both MAC and routing. For the transport function, equal focus can be given to QoS requirements and energy efficiency. Thus an end-to-end solution such as the ART protocol suffices.

5) Alerting system: Alerting systems function similar to safety systems, but with the difference that no emergency action is required on the event that has triggered the alert. Thus the requirements are reliability, availability and energy efficiency. The MAC design could be similar to ER-MAC with less focus on emergency response and more focus on energy efficiency. For the routing function, the event-based TEEN/APTEEN model is appropriate since alerts are event-based. Alternatively, multipath protocols could be used to increase reliability. For the transport function, event-based centralized ART with both up and down stream reliability is appropriate.

6) Monitoring system: Energy efficiency and load balancing are prime requirements of monitoring systems, since they are required to be collecting data on the deployed field for a long duration. Energy efficient clustering schemes are suitable as a common solution for MAC and routing. HEED is one such clustering protocol with the capability to provide energy efficient networks. The transport function can be skipped for this class of systems, due to reduced reliability requirements.

Our aim with this article was to discuss the wireless sensor networks from an industrial perspective. We have discussed the classification of industrial systems into various classes and applications of WSN in these systems. The common important requirements of industrial systems are discussed briefly and also added in some common requirements which we consider important. This was followed by discussion of state-of-the-art in industrial standards for IWSN and its future prospects. New additions like the GINSENG project have been discussed. Security function is discussed in the perspective of its treatment in the industrial standards. We have then discussed various functions like medium access control, routing and transport which are the driving force in satisfying the requirements of the industrial systems. Along with some function specific requirements for each of these functions, we have discussed some representative protocols that aim to meet the requirements set by the various classes of industrial systems and which can be suitably modified to fit into the industrial standards. We have also summarized the classes and protocols that meet requirements for each of the considered classes. These protocols are representative protocols for the requirements they satisfy.

Among the wireless standards discussed, wirelessHART is currently the standard that is widely deployed and companies are more probable to choose wirelessHART when designing a new industrial network. But limited research has been done in the area of routing protocols, transport protocols, and problems of synchronization in the context of wirelessHART. The centralized architecture of wirelessHART, where a network manager [13] is responsible for slot allocation, synchronization and routing can be seen as a single point of failure as we discussed earlier. Hence decentralized solutions with the use of well-known clustering protocols like HEED [110], LEACH [109] can be an interesting area of research. Latency also remains an open issue to be investigated. The attempts to converge wirelessHART and ISA100.11a are a promising way to get the research in this area focused.

Wireless Sensor and Actuator Networks is a fast growing area within IWSN and is now developing as a separate research field. WSAN have specific and often orthogonal requirements that need to be full-filled and also the hardware used is different from the traditional IWSN. There is a need

to create standards specifically for this class of networks and also new protocols need to be developed. Clearly, creating an industrial standard for WSAN solution from scratch is a tedious and time consuming task, and hence it would also be interesting to study the applicability of the current state-of-the-art in industrial standards like wirelessHART, in particular to WSAN. There is a need to study the changes required to these standards in order to satisfy the requirements of WSAN.

ACKNOWLEDGMENT

We are grateful for the comments from the reviewers of IEEE Communications Surveys and Tutorials team that have helped us to improved the paper.

REFERENCES

[1] B. Warneke and K. Pister, "MEMS for distributed wireless sensor networks," in *Proc. 9th Int. Conf. on Electronics, Circuits and Systems*, vol. 1, pp. 291–294, 2002.

[2] I. Khemapech, I. Duncan, and A. Miller, "A survey of wireless sensor networks technology," in *Proc. 6th Annu. Postgraduate Symp. on the Convergence of Telecommunications, Networking and Broadcasting*, 2005.

[3] K. Romer and F. Mattern, "The design space of wireless sensor networks," *IEEE Wireless Commun.*, vol. 11, pp. 54–61, Dec 2004.

[4] I. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: a survey," *Computer Networks*, vol. 38, no. 4, pp. 393–422, 2002.

[5] X. Shen, Z. Wang, and Y. Sun, "Wireless sensor networks for industrial applications," in *Proc. 5th World Congress on Intelligent Control and Automation*, vol. 4, pp. 3636–3640, June 2004.

[6] B. Galloway and G. Hancke, "Introduction to industrial control networks," *IEEE Commun. Surveys & Tutorials*, vol. PP, no. 99, pp. 1–21, 2012.

[7] L. Krishnamurthy, R. Adler, P. Buonadonna, J. Chhabra, M. Flanigan, N. Kushalnagar, L. Nachman, and M. Yarvis, "Design and deployment of industrial sensor networks: experiences from a semiconductor plant and the north sea," in *Proc. 3rd Int. Conf. on Embedded Networked Sensor Systems*, SenSys '05, (New York, NY, USA), pp. 64–75, ACM, 2005.

[8] I. F. Akyildiz and I. H. Kasimoglu, "Wireless sensor and actor networks: research challenges," *Ad Hoc Networks*, vol. 2, no. 4, pp. 351–367, 2004.

[9] H. Salarian, K.-W. Chin, and F. Naghdy, "Coordination in wireless sensor-actuator networks: A survey," *J. of Parallel and Distributed Computing*, vol. 72, no. 7, pp. 856–867, 2012.

[10] Z. Alliance, "Zigbee specification," in *Zigbee Document 053474r13*, Zigbee Alliance, May 2008.

[11] I. W. W. Group, "Draft standard ISA100. 11a," in *Internal working draft*, International Society of Automation, May 2008.

[12] "www.industrialwireless.cn/en/06.asp." Chinese Industrial Wireless Alliance.

[13] D. Chen, M. Nixon, and A. Mok, *WirelessHART: Real-Time Mesh Network for Industrial Automation*. Springer Publishing Company, Incorporated, 1st ed., 2010.

[14] H. Karl and A. Willig, *Protocols and architectures for wireless sensor networks*. Wiley-Interscience, 2007.

[15] J.-P. Vasseur and A. Dunkels, *Interconnecting smart objects with ip: The next internet*. Morgan Kaufmann, 2010.

[16] A. Bachir, M. Dohler, T. Watteyne, and K. Leung, "MAC essentials for wireless sensor networks," *IEEE Commun. Surveys & Tutorials*, vol. 12, no. 2, pp. 222–248, 2010.

[17] V. Sachan, S. Imam, and M. Beg, "Energy-efficient communication methods in wireless sensor networks: A critical review," *Int. J. of Computer Applications*, vol. 39, no. 17, 2012.

[18] J. Al-Karaki and A. Kamal, "Routing techniques in wireless sensor networks: a survey," *IEEE Wireless Commun.*, vol. 11, pp. 6–28, Dec 2004.

[19] C. Wang, K. Sohraby, B. Li, M. Daneshmand, and Y. Hu, "A survey of transport protocols for wireless sensor networks," *IEEE Network*, vol. 20, pp. 34–40, May-June 2006.

[20] J. Yick, B. Mukherjee, and D. Ghosal, "Wireless sensor network survey," *Computer Networks*, vol. 52, no. 12, pp. 2292–2330, 2008.

[21] K. K. II and P. Mohapatra, "Medium access control in wireless sensor networks," *Computer Networks*, vol. 51, no. 4, pp. 961–994, 2007.

[22] I. Demirkol, C. Ersoy, and F. Alagoz, "MAC protocols for wireless sensor networks: a survey," *IEEE Commun. Mag.*, vol. 44, pp. 115–121, April 2006.

[23] K. Langendoen, "Medium access control in wireless sensor networks," *Medium access control in wireless networks*, vol. 2, pp. 535–560, 2008.

[24] Y. Z. Zhao, C. Miao, M. Ma, J. B. Zhang, and C. Leung, "A survey and projection on medium access control protocols for wireless sensor networks," *ACM Computing Surveys*, vol. 45, pp. 7:1–7:37, Dec 2012.

[25] K. Akkaya and M. Younis, "A survey on routing protocols for wireless sensor networks," *Ad Hoc Networks*, vol. 3, no. 3, pp. 325–349, 2005.

[26] T. Watteyne, A. Molinaro, M. Richichi, and M. Dohler, "From MANET to IETF ROLL standardization: A paradigm shift in WSN routing protocols," *IEEE Commun. Surveys & Tutorials*, vol. 13, no. 4, pp. 688–707, 2011.

[27] A. Rathnayaka and V. M. Potdar, "Wireless sensor network transport protocol: A critical review," *J. of Network and Computer Applications*, vol. 36, no. 1, pp. 134–146, 2011.

[28] Z. Teng and K. Kim, "A survey on real-time MAC protocols in wireless sensor networks," *Commun. and Netw.*, vol. 2, no. 2, pp. 104–112, 2010.

[29] P. Suriyachai, U. Roedig, and A. Scott, "A survey of MAC protocols for mission-critical applications in wireless sensor networks," *IEEE Commun. Surveys & Tutorials*, vol. 14, no. 2, pp. 240–264, 2012.

[30] V. Gungor and G. Hancke, "Industrial wireless sensor networks: Challenges, design principles, and technical approaches," *IEEE Trans. Ind. Electron.*, vol. 56, pp. 4258–4265, Oct 2009.

[31] D. Christin, P. S. Mogre, and M. Hollick, "Survey on wireless sensor network technologies for industrial automation: The security and quality of service perspectives," *Future Internet*, vol. 2, no. 2, pp. 96–125, 2010.

[32] L. Hou and N. Bergmann, "System requirements for industrial wireless sensor networks," in *Proc. IEEE Conf. on Emerging Technologies and Factory Automation (ETFA*, pp. 1–8, Sept 2010.

[33] P. Zand, S. Chatterjea, K. Das, and P. Havinga, "Wireless industrial monitoring and control networks: The journey so far and the road ahead," *J. of Sensor and Actuator Networks*, vol. 1, no. 2, pp. 123–152, 2012.

[34] L. Zheng, "Industrial wireless sensor networks and standardizations: The trend of wireless sensor networks for process autometion," in *Proc. SICE Annu. Conf.*, pp. 1187–1190, Aug 2010.

[35] I. Akyildiz and I. Kasimoglu, "A protocol suite for wireless sensor and actor networks," in *Proc. IEEE Radio and Wireless Conf.*, pp. 11–14, Sept 2004.

[36] X. Shen, Z. Wang, and Y. Sun, "Wireless sensor networks for industrial applications," in *5th World Congress on Intelligent Control and Automation*, vol. 4, pp. 3636–3640, 2004.

[37] J. Rabaey, M. Ammer, J. da Silva, J.L., D. Patel, and S. Roundy, "Picoradio supports ad hoc ultra-low power wireless networking," *Computer*, vol. 33, pp. 42–48, Jul 2000.

[38] K. Sha, W. Shi, and O. Watkins, "Using wireless sensor networks for fire rescue applications: Requirements and challenges," in *IEEE Int. Conf. on Electro/information Technol.*, pp. 239–244, 2006.

[39] H. Hashemian, "Aging management of instrumentation & control sensors in nuclear power plants," *Nuclear Engineering and Design*, vol. 240, no. 11, pp. 3781–3790, 2010.

[40] H. Hashemian, "Wireless sensors for predictive maintenance of rotating equipment in research reactors," *Annals of Nuclear Energy*, vol. 38, pp. 665–680, 2011.

[41] A. Flammini, D. Marioli, E. Sisinni, A. Taroni, and M. Pezzotti, "A wireless thermocouples network for temperature control in plastic machinery," in *IEEE Int. Workshop on Factory Commun. Syst.*, pp. 219–222, 2006.

[42] R. Bayindir and Y. Cetinceviz, "A water pumping control system with a programmable logic controller (plc) and industrial wireless modules for industrial plants – an experimental setup," *ISA Transactions*, vol. 50, no. 2, pp. 321–328, 2011.

[43] J. Neander, M. Nolin, M. Bjorkman, S. Svensson, and T. Lennvall, "Wireless vibration monitoring (wivib) - an industrial case study," in *IEEE Int. Conf. on Emerging Technologies and Factory Automation*, pp. 920–923, 2007.

[44] S. Carlsen, A. Skavhaug, S. Petersen, and P. Doyle, "Using wireless sensor networks to enable increased oil recovery," in *IEEE Int. Conf. on Emerging Technologies and Factory Automation*, pp. 1039–1048, 2008.

[45] J. Werb, M. Newman, V. Berry, S. Lamb, D. Sexton, and M. Lapinski, "Improved quality of service in IEEE 802.15. 4 mesh networks," in

Proc. Int. Workshop on Wireless and Industrial Automation, March 2005.

[46] A. Willig, K. Matheus, and A. Wolisz, "Wireless technology in industrial networks," *Proc. IEEE*, vol. 93, pp. 1130–1151, June 2005.

[47] A. Sikora and V. Groza, "Coexistence of IEEE 802.15.4 with other systems in the 2.4 GHz-ISM-band," in *Proc. IEEE Instrumentation and Measurement Technol. Conf.(IMTC)*, vol. 3, pp. 1786–1791, May 2005.

[48] B. Deb, S. Bhatnagar, and B. Nath, "ReInForM: reliable information forwarding using multiple paths in sensor networks," in *Proc. 28th Annu. IEEE Int. Conf. on Local Computer Netw.*, pp. 406–415, Oct 2003.

[49] D. Chen and P. Varshney, "QoS support in wireless sensor networks: A survey," in *Proc. Int. Conf. on Wireless Netw. (ICWN)*, vol. 1, (Las Vegas, Nevada, USA), pp. 227–233, June 2004.

[50] E. Oyman and C. Ersoy, "Multiple sink network design problem in large scale wireless sensor networks," in *Proc. IEEE Int. Conf. Commun.*, vol. 6, pp. 3663–3667, June 2004.

[51] R. Oliver and G. Fohler, "Timeliness in wireless sensor networks: Common misconceptions," in *Proc. 9th Int. Workshop on Real-Time Networks RTN*, 2010.

[52] M. Imran, A. Said, and H. Hasbullah, "A survey of simulators, emulators and testbeds for wireless sensor networks," in *Proc. Int. Symp. in Information Technology (ITSim)*, vol. 2, pp. 897–902, June 2010.

[53] T. Johnson, "Designing a distributed queue," in *Proc. 7th IEEE Symp. on Parallel and Distributed Processing*, pp. 304–311, Oct 1995.

[54] P. Hu and L. Kleinrock, "An analytical model for wormhole routing with finite size input buffers," in *Proc. 15th Int. Teletraffic Congress*, pp. 549–560, June 1997.

[55] G. P. Halkes and K. G. Langendoen, "Experimental evaluation of simulation abstractions for wireless sensor network MAC protocols," *EURASIP J. Wireless Commun. Netw.*, vol. 24, pp. 24:1–24:2, April 2010.

[56] G. Wittenburg and J. Schiller, "A quantitative evaluation of the simulation accuracy of wireless sensor networks," in *Proc. 6th Fachgesprch Drahtlose Sensornetze der GI/ITG-Fachgruppe Kommunikation und Verteilte Systeme*, (Aachen, Germany), pp. 23–26, July 2007.

[57] U. M. Colesanti, C. Crociani, and A. Vitaletti, "On the accuracy of OMNET++ in the wireless sensornetworks domain: simulation vs. testbed," in *Proc. 4th ACM Workshop on Performance evaluation of Wireless Ad Hoc, Sensor,and Ubiquitous Networks*, PE-WASUN '07, (New York, NY, USA), pp. 25–31, ACM, 2007.

[58] "http://www.wina.org/." Wireless Industrial Networking Alliance.

[59] "http://www.zigbee.org/." ZigBee Alliance.

[60] "http://www.hartcomm.org/." wirelessHART datasheets, HART Communication Foundation.

[61] "http://www.isa.org/." The International Society of Automation.

[62] "www.ict-ginseng.eu." GINSENG Project.

[63] K. S. J. Pister and L. Doherty, "TSMP: Time synchronized mesh protocol," in *Proc. IASTED Int. Symp. on Distributed Sensor Netw.*, Nov 2008.

[64] "http://www.dustnetworks.com/." Dust Networks.

[65] H. Hayashi, T. Hasegawa, and K. Demachi, "Wireless technology for process automation," in *Proc. ICCAS-SICE*, pp. 4591–4594, Aug 2009.

[66] W. Liang, X. Zhang, Y. Xiao, F. Wang, P. Zeng, and H. Yu, "Survey and experiments of WIA-PA specification of industrial wireless network," *Wireless Communications and Mobile Computing*, vol. 11, no. 8, pp. 1197–1212, 2011.

[67] T. O'Donovan, J. Brown, U. Roedig, C. Sreenan, J. Do Ó and, A. Dunkels, A. Klein, Sa, J. Silva, V. Vassiliou, and L. Wolf, "GINSENG: Performance control in wireless sensor networks," in *Proc. 7th Annu. IEEE Commun. Society Conf. on Sensor Mesh and Ad Hoc Commun. and Netw. (SECON)*, pp. 1–3, june 2010.

[68] P. Suriyachai, J. Brown, and U. Roedig, "Time-critical data delivery in wireless sensor networks," in *Proc. Int. Conf. on Distributed Computing in Sensor Systems*, vol. 6131, pp. 216–229, Springer Berlin Heidelberg, 2010.

[69] F. Busching, W. Pottner, D. Brokelmann, G. von Zengen, R. Hartung, K. Hinz, and L. Wolf, "A demonstrator of the GINSENG-approach to performance and closed loop control in WSNs," in *Proc. 9th Int. Conf. on Networked Sensing Systems (INSS)*, pp. 1–2, June 2012.

[70] S. Petersen and S. Carlsen, "WirelessHART versus ISA100.11a: The format war hits the factory floor," *IEEE Ind. Electron. Mag.*, vol. 5, pp. 23–34, Dec 2011.

[71] A. Perrig, J. Stankovic, and D. Wagner, "Security in wireless sensor networks," *ACM Commun.*, vol. 47, pp. 53–57, June 2004.

[72] P. Radmand, A. Talevski, S. Petersen, and S. Carlsen, "Taxonomy of wireless sensor network cyber security attacks in the oil and gas industries," in *Advanced Information Networking and Applications (AINA), 2010 24th IEEE Int. Conf.*, pp. 949–957, 2010.

[73] Y. Wang, G. Attebury, and B. Ramamurthy, "A survey of security issues in wireless sensor networks," *IEEE Commun. Surveys & Tutorials*, vol. 8, no. 2, pp. 2–23, 2006.

[74] J. P. Walters, Z. Liang, W. Shi, and V. Chaudhary, "Wireless sensor network security: A survey," *Security in distributed, grid, mobile, and pervasive computing*, vol. 1, 2006.

[75] X. Chen, K. Makki, K. Yen, and N. Pissinou, "Sensor network security: a survey," *IEEE Commun. Surveys & Tutorials*, vol. 11, no. 2, pp. 52–73, 2009.

[76] J. Sen, "A survey on wireless sensor network security," *Int. J. of Commun. Netw. and Information Security*, vol. 1, pp. 55–78, August 2009.

[77] T. OḎonovan, J. Brown, F. Buesching, A. Cardoso, J. Cecilio, J. Do Ó, P. Furtado, P. Gil, A. Jugel, W. B. Pöttner, U. Roedig, J. Sá silva, R. Silva, C. J Sreenan, V. Vassiliou, T. Voigt, L. Wolf, and Z. Zinonos, "The GINSENG System for Wireless Monitoring and Control: Design and Deployment Experiences," *ACM Trans. on Sensor Netw.*, vol. 10, no. 3, 2014. (To appear).

[78] N. Abramson, "Development of the ALOHANET," *IEEE Trans. Inf. Theory*, vol. 31, pp. 119–123, Mar 1985.

[79] I. Rhee, A. Warrier, M. Aia, J. Min, and M. L. Sichitiu, "Z-MAC: a hybrid MAC for wireless sensor networks," *IEEE/ACM Trans. Netw.*, vol. 16, pp. 511–524, June 2008.

[80] L. Sitanayah, C. J. Sreenan, and K. N. Brown, "Emergency response MAC protocol (ER-MAC) for wireless sensor networks," in *Proc. 9th ACM/IEEE Int. Conf. Information Processing in Sensor Netw.*, IPSN '10, (New York, NY, USA), pp. 364–365, ACM, 2010.

[81] C. Cano, B. Bellalta, A. Sfairopoulou, and M. Oliver, "Low energy operation in WSNs: A survey of preamble sampling MAC protocols," *Computer Networks*, vol. 55, no. 15, pp. 3351–3363, 2011.

[82] S. Coleri, A. Puri, and P. Varaiya, "Power efficient system for sensor networks," in *Proc. 8th IEEE Int. Symp. on Computers and Commun.*, vol. 2, pp. 837–842, June-July 2003.

[83] S. Kulkarni, "Tdma service for sensor networks," in *Distributed Computing Systems Workshops, 2004. Proc. 24th Int. Conf.*, pp. 604–609, 2004.

[84] S. Kulkarni, "TDMA service for sensor networks," in *Proc. 24th Int. Conf. on Distributed Computing Systems Workshops*, pp. 604–609, March 2004.

[85] V. Cionca, T. Newe, and V. Dadarlat, "TDMA protocol requirements for wireless sensor networks," in *Proc. 2nd Int. Conf. on Sensor Technologies and Applications*, pp. 30–35, aug. 2008.

[86] L. Doherty and D. A. Teasdale, "Towards 100% reliability in wireless monitoring networks," in *Proc. 3rd ACM Int. Workshop on Performance Evaluation of Wireless ad hoc, sensor and ubiquitous networks*, PE-WASUN '06, (New York, NY, USA), pp. 132–135, ACM, 2006.

[87] J. Elson and K. Römer, "Wireless sensor networks: a new regime for time synchronization," *ACM SIGCOMM Computer Commun. Review*, vol. 33, pp. 149–154, Jan. 2003.

[88] M. Nunes, A. Grilo, and M. Macedo, "Interference-free TDMA slot allocation in wireless sensor networks," in *Proc. 32nd IEEE Conf. on Local Comput. Netw.*, pp. 239–241, Oct 2007.

[89] J. Elson and D. Estrin, "Time synchronization for wireless sensor networks," in *Proc. 15th Int. Workshop on Parallel and Distributed Processing Symp.*, pp. 1965–1970, April 2001.

[90] Q. Li and D. Rus, "Global clock synchronization in sensor networks," *IEEE Trans. Comput.*, vol. 55, pp. 214–226, Feb 2006.

[91] O. D. Incel, "A survey on multi-channel communication in wireless sensor networks," *Computer Networks*, vol. 55, no. 13, pp. 3081–3099, 2011.

[92] T. Melodia, M. Vuran, and D. Pompili, "The state of the art in cross-layer design for wireless sensor networks," in *Wireless Systems and Network Architectures in Next Generation Internet* (M. Cesana and L. Fratta, eds.), vol. 3883 of *Lecture Notes in Computer Science*, pp. 78–92, Springer Berlin Heidelberg, 2006.

[93] N. Chilamkurti, S. Zeadally, A. Vasilakos, and V. Sharma, "Cross-layer support for energy efficient routing in wireless sensor networks," *J. of Sensors*, vol. 2009, 2009.

[94] Y. Li, C. S. Chen, Y.-Q. Song, and Z. Wang, "Real-time QoS support in wireless sensor networks: a survey," in *Proc. 7th IFAC Int. Conf. on Fieldbuses & Networks in Industrial & Embedded Systems - FeT'2007*, (Toulouse, France), 2007.

[95] P. Huang, L. Xiao, S. Soltani, M. Mutka, and N. Xi, "The evolution of MAC protocols in wireless sensor networks: A survey," *IEEE Commun. Surveys & Tutorials*, vol. PP, no. 99, pp. 1–20, 2012.

[96] B. Yahya and J. Ben-Othman, "Towards a classification of energy aware MAC protocols for wireless sensor networks," *Wireless Commun. and Mobile Computing*, vol. 9, no. 12, pp. 1572–1607, 2009.

[97] M. Al Ameen, S. Islam, and K. Kwak, "Energy saving mechanisms for MAC protocols in wireless sensor networks," *Int. J. of Distributed Sensor Netw.*, vol. 2010, 2010.

[98] G. Anastasi, M. Conti, M. D. Francesco, and A. Passarella, "Energy conservation in wireless sensor networks: A survey," *Ad Hoc Networks*, vol. 7, no. 3, pp. 537–568, 2009.

[99] M. A. Yigitel, O. D. Incel, and C. Ersoy, "QoS-aware MAC protocols for wireless sensor networks: A survey," *Computer Networks*, vol. 55, no. 8, pp. 1982–2004, 2011.

[100] J. Chen, M. Daz, L. Llopis, B. Rubio, and J. M. Troya, "A survey on quality of service support in wireless sensor and actor networks: Requirements and challenges in the context of critical infrastructure protection," *J. of Network and Computer Applications*, vol. 34, no. 4, pp. 1225–1239, 2011.

[101] P. Suriyachai, U. Roedig, and A. Scott, "Implementation of a MAC protocol for QoS support in wireless sensor networks," in *Proc. IEEE Conf. on Pervasive Comput. and Commun.*, pp. 1–6, march 2009.

[102] L. Sitanayah, C. Sreenan, and K. Brown, "ER-MAC: A hybrid MAC protocol for emergency response wireless sensor networks," in *Proc. 4th Int. Conf. on Sensor Technologies and Applications (SENSORCOMM)*, pp. 244–249, July 2010.

[103] W. Z. Khan, N. M. Saad, and M. Y. Aalsalem, "An overview of routing metrics for the evaluation of routing protocols in wireless sensor networks," *European J. of Scientific Research*, vol. 79, no. 2, pp. 208–224, 2012.

[104] K. Pister, P. Thubert, C. Systems, S. Dwars, and T. Phinney, "Industrial routing requirements in low-power and lossy networks," 2009.

[105] J. Vasseur, M. Kim, K. Pister, N. Dejean, and D. Barthel, "Routing metrics used for path calculation in low power and lossy networks," *Internet Draft*, March 2011.

[106] K. Sohrabi, J. Gao, V. Ailawadhi, and G. Pottie, "Protocols for self-organization of a wireless sensor network," *IEEE Pers. Commun.*, vol. 7, pp. 16–27, Oct 2000.

[107] C. Intanagonwiwat, R. Govindan, and D. Estrin, "Directed diffusion: a scalable and robust communication paradigm for sensor networks," in *Proc. 6th annu. Int. Conf. on Mobile computing and networking*, MobiCom, (New York, NY, USA), pp. 56–67, ACM, 2000.

[108] A. A. Abbasi and M. Younis, "A survey on clustering algorithms for wireless sensor networks," *Computer Communications*, vol. 30, pp. 2826–2841, 2007.

[109] W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy-efficient communication protocol for wireless microsensor networks," in *Proc. 33rd Annu. Hawaii Int. Conf. on System Sciences*, vol. 2, Jan 2000.

[110] O. Younis and S. Fahmy, "HEED: A hybrid, energy-efficient, distributed clustering approach for ad hoc sensor networks," *IEEE Trans. Mobile Comput.*, vol. 3, pp. 366–379, Oct-Dec 2004.

[111] A. Manjeshwar and D. Agrawal, "TEEN: A routing protocol for enhanced efficiency in wireless sensor networks," in *Proc. 15th Int. Parallel and Distrib. Processing Symp.*, IPDPS, April 2001.

[112] K. Chandrimima Rahman, "A survey on sensor network," *J. of Computer and Information Technology*, vol. 1, pp. 76–87, 2010.

[113] S. K. Singh, M. P. Singh, and D. K. Singh, "A survey of energy-efficient hierarchical cluster-based routing in wireless sensor networks," *Int. J. of Advanced Networking and Applications*, vol. 2, pp. 570–580, 2010.

[114] V. Quang and T. Miyoshi, "Adaptive routing protocol with energy efficiency and event clustering for wireless sensor networks," *IEICE Trans. Commun.*, vol. 91, no. 9, pp. 2795–2805, 2008.

[115] J. Neander, E. Hansen, M. Nolin, and M. Bjorkman, "Asymmetric multihop communication in large sensor networks," in *Proc. 1st Int. Symp. on Wireless Pervasive Computing*, Jan 2006.

[116] M. Hammoudeh, A. Kurz, and E. Gaura, "MuMHR: Multi-path, multi-hop hierarchical routing," in *Proc. Int. Conf. on Sensor Technologies and Applications*, SensorComm, pp. 140–145, Oct 2007.

[117] T. He, J. Stankovic, C. Lu, and T. Abdelzaher, "SPEED: a stateless protocol for real-time communication in sensor networks," in *Proc. 23rd Int. Conf. on Distributed Computing Syst.*, pp. 46–55, May 2003.

[118] E. Felemban, C.-G. Lee, and E. Ekici, "MMSPEED: multipath multi-speed protocol for qos guarantee of reliability and timeliness in wireless sensor networks," *IEEE Trans. Mobile Comput.*, vol. 5, pp. 738–754, June 2006.

[119] S. Mueller, R. Tsang, and D. Ghosal, "Multipath routing in mobile ad hoc networks: Issues and challenges," in *Performance Tools and Applications to Networked Systems* (M. Calzarossa and E. Gelenbe, eds.), vol. 2965 of *Lecture Notes in Computer Science*, pp. 209–234, Springer Berlin Heidelberg, 2004.

[120] F. Ye, A. Chen, S. Lu, and L. Zhang, "A scalable solution to minimum cost forwarding in large sensor networks," in *Proc. 10th Int. Conf. on Computer Commun. and Netw.*, pp. 304–309, 2001.

[121] D. Ganesan, R. Govindan, S. Shenker, and D. Estrin, "Highly-resilient, energy-efficient multipath routing in wireless sensor networks," *ACM SIGMOBILE Mobile Computing and Commun. Review*, vol. 5, pp. 11–25, Oct 2001.

[122] H. Alwan and A. Agarwal, "A survey on fault tolerant routing techniques in wireless sensor networks," in *Proc. 3rd Int. Conf. on Sensor Technologies and Applications*, SENSORCOMM, pp. 366–371, June 2009.

[123] H. Hassanein and J. Luo, "Reliable energy aware routing in wireless sensor networks," in *Proc. 2nd IEEE Workshop on Dependability and Security in Sensor Networks and Systems*, pp. 54–64, April 2006.

[124] T. Winter, P. Thubert, A. Brandt, J. Hui, R. Kelsey, P. Levis, K. Pister, R. Stuik, J. Vasseur, and R. Alexander, "RPL: Ipv6 routing protocol for low-power and lossy networks," *Internet Draft*, March 2012.

[125] J. Tripathi, J. de Oliveira, and J. Vasseur, "Performance evaluation of routing protocol for low power and lossy networks (RPL)," *Internet Draft*, August 2011.

[126] J. Ko, S. Dawson-Haggerty, and O. Gnawali, "Evaluating the performance of RPL and 6LoWPAN in tinyOS," in *Proc. Int. Conf. on Information Processing for Sensor Networks, ACM*, (Chicago, Illinois), April 2011.

[127] N. Accettura, L. Grieco, G. Boggia, and P. Camarda, "Performance analysis of the rpl routing protocol," in *Proc. IEEE Int. Conf. on Mechatronics (ICM)*, pp. 767–772, April 2011.

[128] T. Clausen, U. Herberg, and M. Philipp, "A critical evaluation of the IPv6 routing protocol for low power and lossy networks (RPL)," in *Proc. IEEE 7th Int. Conf. on Wireless and Mobile Computing, Networking and Commun. (WiMob)*, pp. 365–372, Cct 2011.

[129] A. Manjeshwar and D. Agrawal, "APTEEN: A hybrid protocol for efficient routing and comprehensive information retrieval in wireless sensor networks," in *Proc. 16th Int. Parallel and Distributed Processing Symp.*, p. 48, 2002.

[130] K. Sharma, A. Rathor, S. Biradar, and M. Ghose, "Power-efficient routing & increased yield approach for WSNs," *Int. J. on Computer Science and Engineering*, vol. 2, pp. 586–592, 2010.

[131] V. C. Gungor, O. B. Akan, and I. F. Akyildiz, "A real-time and reliable transport $(\mathrm{RT})^2$ protocol for wireless sensor and actor networks," *IEEE/ACM Trans. Netw.*, vol. 16, pp. 359–370, April 2008.

[132] N. Tezcan and W. Wang, "ART; an asymmetric and reliable transport mechanism for wireless sensor networks," *Int. J. of Sensor Networks*, vol. 2, pp. 188–200, April 2007.

[133] H. Zhang, A. Arora, Y.-R. Choi, and M. G. Gouda, "Reliable bursty convergecast in wireless sensor networks," *Computer Communications*, vol. 30, no. 13, pp. 2560–2576, 2007.

[134] B. Hull, K. Jamieson, and H. Balakrishnan, "Mitigating congestion in wireless sensor networks," in *Proc. 2nd Int. Conf. on Embedded networked sensor systems*, SenSys '04, (New York, NY, USA), pp. 134–147, ACM, 2004.

[135] M. Mahmood and W. Seah, "Reliability in wireless sensor networks: Survey and challenges ahead," tech. rep., Victoria University of Wellington, Febraury 2012. Last accessed on August 22, 2012.

[136] F. Stann and J. Heidemann, "RMST: Reliable data transport in sensor networks," in *Proc. 1st IEEE. 2003 IEEE Int. Workshop on Sensor Network Protocols and Applications*, pp. 102–112, May 2003.

[137] C.-Y. Wan, A. T. Campbell, and L. Krishnamurthy, "PSFQ: A reliable transport protocol for wireless sensor networks," in *Proc.1st ACM Int. Workshop on Wireless Sensor Networks and Applications*, WSNA '02, (New York, NY, USA), pp. 1–11, ACM, 2002.

[138] P. Pereira, A. Grilo, F. Rocha, M. Nunes, A. Casaca, C. Chaudet, P. Almström, and M. Johansson, "End-to-end reliability in wireless sensor networks: Survey and research challenges," in *Proc. EuroFGI Workshop on IP QoS and Traffic Control*, pp. 67–74, 2007.

[139] J. Akerberg, M. Gidlund, and M. Bjorkman, "Future research challenges in wireless sensor and actuator networks targeting industrial automation," in *Proc. 9th IEEE Int. Conf. on Industrial Informatics (INDIN)*, pp. 410–415, July 2011.

[140] C. De Dominicis, P. Ferrari, A. Flammini, E. Sisinni, M. Bertocco, G. Giorgi, C. Narduzzi, and F. Tramarin, "Investigating wirelesshart coexistence issues through a specifically designed simulator," in *Proc.*

Int. Conf. on IEEE Instrumentation and Measurement Technology, pp. 1085–1090, May 2009.

[141] P. Ciciriello, L. Mottola, and G. Picco, "Efficient routing from multiple sources to multiple sinks in wireless sensor networks," *Wireless Sensor Networks*, vol. 4373, pp. 34–50, 2007.

[142] T. Melodia, D. Pompili, V. Gungor, and I. Akyildiz, "Communication and coordination in wireless sensor and actor networks," *IEEE Trans. Mobile Comput.*, vol. 6, pp. 1116–1129, Oct 2007.

A. Ajith Kumar S. received double Masters with M.Sc in computer science from the Eindhoven University of Technology (Netherlands) and M.Tech in Software Engineering from Manipal Institute of Technology (India) in 2011 funded partly by the Eindhoven University of Technology. He is currently employed for a doctorate position in Bergen University College (Norway) in the faculty of engineering in a collaboration project between the computer science and electrical engineering. The project involves modeling and verification from the computer science side and wireless sensor network from the electrical engineering. Has previously worked in the Embedded Systems Institute in Eindhoven, the Netherland for his masters project. The project involved extension of the Design Space Exploration project which produced the Octopus toolset. His research interests include modeling and verification, real-time systems, wireless sensor actuator networks and software engineering in general.

Knut Øvsthus received his MS from The Norwegian University of Science and Technology (NTNU) and PhD for University of Oslo. He started his career at Telenor R&D in 1987 where he initially did research on semiconductor lasers. The PhD included both experimental work as well as theoretical work. Following the changes in the telecom industry, his research changed towards network technology focusing on IP-based networks. He initiated and took part in management of European research projects in this area. In 2001 he joined the Norwegian Defense Research Establishment, and was given the responsibility of managing a large research project in communication network. From 2006 he has been a professor at Bergen University College. His research interest is WSN and its usage in industrial networks, healthcare, conditioning monitoring and environmental monitoring.

Lars M. Kristensen received the PhD in computer science from the University of Aarhus (Denmark), and is currently professor in software engineering at Bergen University College (Norway) where he is director of a strategic research programme on software technologies for distributed systems. Upon the completion of his PhD, he worked as a post-doctoral researcher in computer systems engineering at University of South Australia and the Australian Defence Science and Technology Organisation concentrating on implementation of software tools for military planning and on the development of real-time avionics mission systems. Following the post-doctoral research position, he obtained a permanent position at University of Aarhus and was involved in a number of industry supported research projects within modelling and validation of Internet protocols, mobile ad-hoc networks, and sensor networks. He has published more than 70 papers in strictly refereed journals and conference proceedings, is a regular member of technical PCs within distributed systems and software engineering, is member of the Editorial Board of the TopNoC Springer journal, and is a member of the steering committee for the International Petri Nets conference. He is co-author of the most recent textbook on Coloured Petri Net and CPN Tools which is one of the most widely used academic software tools for modelling and validation of concurrent systems. In 2007 he received the Danish Research Councils Young Researchers Award.