OTTO VON GUERICKE
UNIVERSITÄT
MAGDEBURG

FACULTY OF
COMPUTER SCIENCE

Communication and
Networked Systems

DISSERTATION

Medium Access Control Protocols for Reliable Communication in Low-Power Industrial Applications

Dissertation zur Erlangung des akademischen Grades
Doktoringenieur (Dr.-Ing.) an der Fakultät für Informatik
der Otto-von-Guericke-Universität Magdeburg

Author

Saleem Raza

Reviewers

Prof. Dr. Mesut Güneş

Prof. Dr. Jochen Schiller

Prof. Dr. Torsten Braun

Saleem Raza

Medium Access Control Protocols for Reliable Communication in Low-Power Industrial Applications

Dissertation, Otto-von-Guericke-University Magdeburg, 2019

Medium Access Control Protocols for Reliable Communication
in Low-Power Industrial Applications

DISSERTATION

zur Erlangung des akademischen Grades

Doktoringenieur (Dr.-Ing.)

angenommen durch die Fakultät für Informatik
der Otto-von-Guericke-Universität Magdeburg

vorgelegt von:
M.Ing. Saleem Raza

geb .am 01.01.1985 in Moro, Naushahro Feroze

Gutachterinnen/Gutachter:

Prof. Dr. Mesut Güneș (University of Magdeburg, Germany)
Prof. Dr. Jochen Schiller (Free University of Berlin, Germany)
Prof. Dr. Torsten Braun (University of Bern, Switzerland)

Eingereicht am:
Magdeburg, den 15.11.2019
Verteidigt am:
Magdeburg, den 11.03.2020

Abstract

A Wireless Sensor and Actuator Network (WSAN) is a network of sensors and actuators connected through wireless medium in which sensors transmit the sensed phenomenon to the actuators and actuators act on it. These networks have appealed many of the industrial applications, particularly wireless networked control systems where the whole control loop can be closed through WSAN. These applications require reliable communication together with deterministic delay from sensor to actuators so as to timely control industrial processes and systems. In this way, they impose severe constraints on reliability, latency, scalability, adaptivity, and energy consumption. Mostly, such constraints can be addressed by the Medium Access Control (MAC) layer, because it can directly control many of the radio related activities such as collisions, retransmissions, interference, and idle-listening.

Therefore, this thesis explores MAC layer and analyzes existing MAC protocols so as to determine to what extent they can satisfy the requirements of low-power industrial applications. In this direction, first we provide a critical analysis of Time-Slotted Channel Hopping (TSCH) MAC protocol, which is considered the most suitable protocol for the Industrial Internet of Things (IIoT) because of its low energy consumption and high reliability claims. Notably, we study the impact of inter-network interference, intra-network interference, and behavior of interaction among closely co-located TSCH networks. To achieve this, we investigate the impact of inter-network interference among networks when introducing a clock drift between them. We analyze the impact of channel hopping on interference by varying the number of available channels in each network. Our results denote that, since TSCH networks are time-synchronized, co-located networks interfere periodically and this period depends on the clock drift among the networks.

Second, we critically analyze TSCH under node mobility, where we denote how mobility can impact reliability of the protocol. Our analysis reveals that mobility can cause significant network downtime where nodes are unable to associate to

the network for long period of time because of synchronization loss, especially if the space is not fully covered by enough nodes. As per our analysis, TSCH can handle mobility well if the network space in which mobile nodes are evolving is fully covered by static nodes or there are enough mobile nodes to maintain a consistent coverage. However, this increases message overhead which causes more delay and energy consumption and thus impacts reliability of the protocol.

Based on our analysis, we propose Dual-Mode Time-Slotted (DMTS)-MAC protocol for industrial process control applications. The DMTS-MAC protocol uses time-slotted structure in a dual-mode together with frequency diversity to satisfy high reliability, low latency, high scalability, and low energy consumption requirements of industrial process control applications. It takes into account the dynamics of process controller and it is adaptive to its varying traffic requirements. The protocol is evaluated through simulations and the results denote that DMTS outperforms existing MAC protocols under several performance metrics.

Zusammenfassung

Ein drahtloses Sensor-und Aktuatorennetzwerk (WSAN) ist ein Netzwerk von Sensoren und Aktoren, die drahtlos kommunizieren, in dem Sensoren das erfasste Phänomen an die Aktoren übertragen und Aktoren darauf reagieren. Diese Netzwerke haben viele industrielle Anwendungen, insbesondere drahtlose vernetzte Steuerungssysteme, bei denen der gesamte Regelkreis über WSAN geschlossen werden kann. Diese Anwendungen erfordern eine zuverlässige Kommunikation zusammen mit einer deterministischen Verzögerung vom Sensor bis zum Aktor, um industrielle Prozesse und Systeme in Echtzeit zu steuern. Auf diese Weise stellen sie erhebliche Anforderungen an Zuverlässigkeit, Latenz, Skalierbarkeit, Anpassungsfähigkeit und Energieverbrauch. Meistens können solche Anforderungen durch die Medium Access Control (MAC)-Schicht adressiert werden, da sie viele der funkbasierten Aktivitäten wie Kollisionen, Wiederholungen, Störungen und unnötiges Zuhören direkt steuern kann.

Diese Arbeit untersucht die MAC-Schicht und analysiert inwieweit bestehende MAC-Potokolle die Anforderungen von industriellen Anwendungen mit geringem Engergieverbrauch erfüllen können. Dazu analysieren wir zunächst das Time Slotted Channel Hopping (TSCH) MAC-Protokoll, das aufgrund seines geringen Energieverbrauchs und seiner hohen Zuverlässigkeitsansprüche als das am besten geeignete Protokoll für das Industrial Internet of Things (IIoT) gilt. Insbesondere untersuchen wir die Auswirkungen von Inter-Netzwerk-Interferenzen, Interferenzen innerhalb des Netzwerks und das Verhalten der Interaktion von nahe gelegenden TSCH-Netzwerken. Dazu untersuchen wir die Auswirkungen von Inter-Netzwerk-Interferenzen zwischen Netzwerken mit herbeigeführtem Taktdrift. Wir analysieren die Auswirkungen von Channel-Hopping auf Störungen durch Variation der Anzahl der verfügbaren Kanäle in jedem Netzwerk. Die Ergebnisse zeigen, dass TSCH-Netzwerke ko-lokalisierte Netzwerke periodisch stören und diese Periode von dem Taktdrift zwischen den Netzwerken abhängt.

Zweitens analysieren wir TSCH auf Knoten-Mobilität, wobei wir angeben, wie

Mobilität die Zuverlässigkeit des Protokolls beeinträchtigen kann. Unsere Analyse zeigt, dass Mobilität zu erheblichen Netzwerkausfällen führen kann, wenn Knoten aufgrund von Synchronisationsverlusten längere Zeit nicht mit dem Netzwerk verbunden werden können, insbesondere wenn der Raum nicht vollständig durch genügend Knoten abgedeckt ist. Gemäß unserer Analyse kann TSCH mit Mobilität gut umgehen, wenn der Raum für das Netzwerk, in dem sich mobile Knoten bewegen, vollständig von statischen Knoten abgedeckt wird oder es genügend mobile Knoten gibt, um eine gleichmäßige Abdeckung aufrechtzuerhalten. Dies erhöht jedoch den Nachrichten-Overhead, was zu mehr Verzögerung und erhöhtem Energieverbrauch führt und somit die Zuverlässigkeit des Protokolls beeinträchtigt.

Basierend auf unserer Analyse schlagen wir das Dual-Mode Time-Slotted (DMTS)-MAC-Protokoll für industrielle Prozesskontrollanwendungen vor. Das DMTS-MAC-Protokoll verwendet eine Zeitschlitzstruktur in Kombination mit Frequenzdiversität, um die hohen Anforderungen an Zuverlässigkeit, geringe Latenzzeiten, hohe Skalierbarkeit und niedrigen Energieverbrauch von industriellen Prozesskontrollanwendungen zu erfüllen. Es berücksichtigt die Dynamik des Prozesskontrollers und dessen Adaptivität zu dem wechselnden Netzwerkverkehr. Das Protokoll wird durch Simulationen ausgewertet und die Ergebnisse deuten darauf hin, dass DMTS bestehende MAC-Protokolle in mehreren Leistungskennzahlen übertrifft.

Dedicated to the loving memory of my parents and brother

Contents

List of Figures

List of Tables

List of Acronyms

DMA-MAC Dual-Mode Adaptive-MAC. xiv, 8, 10, 56, 57, 82, 111–113, 117, 119, 120, 122, 127

DMTS Dual-Mode Time-Slotted. viii, xvi, 7, 10, 75, 80–82, 111–122, 124–127, 132, 133

DSME Deterministic and Synchronous Multi-channel Extension. 38–41

DSSS Direct Sequence Spread Spectrum. 33, 49, 51

EB Enhanced Beacon. 39, 63–65, 87, 88, 100–102

ED Energy Detection. 32, 49

FDMA Frequency Division Multiple Access. 27, 28, 31, 46

FFD Full Function Device. 32, 37

FHSS Frequency Hopping Spread Spectrum. 51

GTS Guaranteed Time Slot. 34, 38–40

IETF Internet Engineering Task Force. 9, 65–67, 69, 72, 78, 102

IIoT Industrial Internet of Things. vii, 3, 7, 9, 11, 66, 67, 69, 85

IoT Internet of Things. 1, 2, 7, 9, 11, 36, 41, 47, 67, 72, 77, 78, 86, 87, 130, 133

ISA International Society of Automation. 19, 43

ISM Industrial Scientific and Medical. 5, 7, 13, 25, 32, 46, 130

IWSAN Industrial Wireless Sensor and Actuator Network. xiii, xvii, 5, 7–11, 15, 16, 18, 19, 21–23, 27, 51, 52, 54, 56, 57, 65, 111, 129

IWSN Industrial Wireless Sensor Network. xiii, xvii, 4, 5, 11, 14–17, 23, 54, 63

KA Keep-Alive. 10, 64, 81, 101, 102, 104–108

LLN Low-Power and Lossy Network. 1, 59, 65, 69, 72, 75, 77, 78, 80

LQI Link Quality Indication. 32, 49

MAC Medium Access Control. vii, viii, xiii, xiv, xvi, xxi, 2, 6–10, 12–14, 21, 23, 25–34, 36–46, 48, 50–52, 54–57, 59–62, 64–68, 71, 75, 77, 80–82, 84, 86, 102, 111–122, 124–127, 129, 130, 132, 133

NCS Networked Control System. 18, 114

PAN Personal Area Network. xv, 32–34, 41, 62, 64, 86, 87, 90, 92, 94, 96

PDR Packet Delivery Ratio. xv, 80, 81, 84, 124, 127

PHY Physical. 2, 9, 14, 25, 31, 32, 37, 43, 46, 49, 57, 75, 130

QoS Quality of Service. 13, 19, 23, 26, 47, 50, 54, 62, 69, 72, 129

RFD Reduced Function Device. 32, 37

RPL IPv6 Routing Protocol for Low-Power and Lossy Networks. xiv, 59, 67, 68, 77, 79, 86, 87, 95, 102

TDMA Time Division Multiple Access. 23, 27, 28, 31, 34, 40, 44, 46, 52, 54, 56, 112–114, 116, 118, 127, 132

TSCH Time-Slotted Channel Hopping. vii, viii, xiv, xv, 7, 9, 10, 41–43, 49, 59–69, 75, 77, 79–82, 85–88, 90–109, 111–113, 122, 124–127, 130, 131, 133

TSMP Time Synchronized Mesh Protocol. 41–43, 113

WLAN Wireless Local Area Network. 3, 11, 48, 50, 51

WPAN Wireless Personal Area Network. 1, 2, 31, 37, 47

WSAN Wireless Sensor and Actuator Network. vii, xiii, 1, 3, 5, 17–19, 26

WSN Wireless Sensor Network. xiii, xvii, 1, 3, 4, 11, 13–19, 23, 26–30, 51, 52, 55

CHAPTER 1

Introduction

THE vision to connect everyday physical objects to the Internet promises to create the Internet of Things (IoT) which is expected to integrate diverse technologies such as sensors, actuators, RFID, communication technologies, and Internet protocols. IoT promises to play a remarkable role in various application domains, such as smart homes [1], medical care [2, 3], industrial automation [4, 5], intelligent transportation [6, 7], resource management [8], smart cities [9, 10], and energy management [11, 12] as denoted in Figure 1.1. For example, in a smart home application, based on user prescribed settings, different monitoring and control tasks are carried out by smart sensors and actuators, such as the heating control system, air-condition monitoring, and fire alarms.

Closely related to the IoT are Machine-to-Machine communication [13], Wireless Sensor Networks (WSNs) [14], Wireless Personal Area Networks (WPANs) [15], Wireless Sensor and Actuator Networks (WSANs) [16, 17], and Cyber-Physical Systems (CPSs) [18, 19], which are application-dependent terms.

Both wired and wireless networks are utilized to support information exchange at the backbone and local access networks. The local access networks, in particular, are wireless, support multi-hop communication, and enable mobility [20]. As these networks are usually low-power and unreliable, they are referred to as Low-Power and Lossy Networks (LLNs) [21]. These networks lay the necessary foundation of IoT and contribute to making it highly accessible. The aspect of ubiquitous accessibility of services and objects to mobile users is imperative because most of the IoT services are targeted to mobile users. Another strong aspect is the autonomous operation, where IoT helps decentralize the decision-making process in order to accomplish autonomous operations with minimal human intervention.

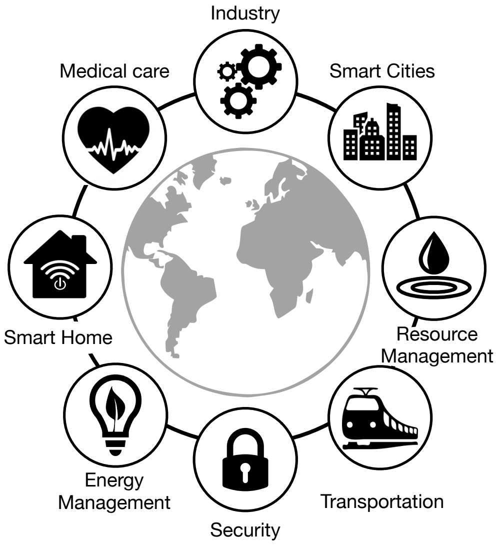


Figure 1.1: Applications of IoT in different domains.

This autonomous feature is of paramount importance for a multitude of industrial applications that enable smart processes and systems. This has amplified the vision of fourth Industrial revolution, also known as the Industry 4.0 [22].

Although IoT seems to revolutionize industries, it is only if it satisfies the strict requirements and challenges that are put in place by industrial applications. Such challenges include: high reliability, low latency, robustness, fault tolerance, scalability, and energy efficiency. In the effort to address such requirements, we witness a vast expansion of the latest wireless standards and technologies based on the WPAN standard IEEE 802.15.4 [23]. The IEEE 802.15.4 primarily targets industrial applications and incorporates significant amendments to previous and existing WPAN standards [24, 25, 26]. As a result, various standards emerged for industrial applications such as Zigbee [27], WirelessHART [28], ISA100.11a [29], 6LoWPAN [30], and WIA-PA [31]. A notable trend in these standards has been a continuous and significant improvement and optimization in the design of Medium Access Control (MAC) protocols so as to meet the aforementioned requirements. This is because MAC influences many of the Physical (PHY) layer aspects of the wireless communication and therefore, it can be utilized to satisfy aforementioned requirements.

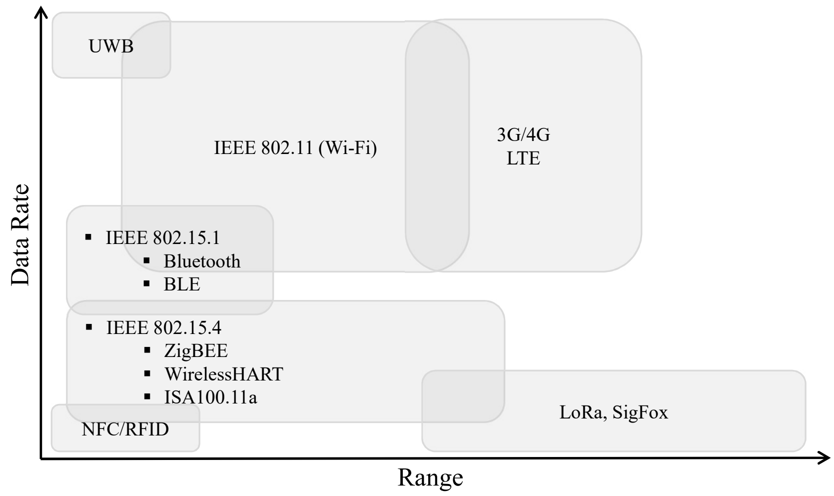


Figure 1.2: Range versus data rate comparison of the low-power wireless standards and technologies.

1.1 Background

During the last decade, wireless technologies have been increasingly utilized in industries, leading to the Industrial Internet of Things (IIoT) mainly driven by low-power standards which have limited range and data rate as compared to traditional Wireless Local Area Network (WLAN) and cellular technologies as depicted in Figure 1.2. The shift from wired to wireless networks dramatically helps reduce huge capital expenditures of installation and maintenance of wires. Moreover, wired networks are rigid and fixed in nature. This makes them difficult to adapt to changes in industrial environments. In addition, certain industrial applications require mobile robots, which becomes a huge challenge with wired networks. However, wireless networks have the capability to support such mobility scenarios.

At the core of the IIoT are the WSNs and Wireless Sensor and Actuator Networks (WSANs). These networks play a central role of connecting machines, parts, products, and humans and create a diverse set of new applications to support intelligent and autonomous decision making.

A WSN is a network of small battery-operated nodes which have the capabilities of sensing, processing, and communication. A typical wireless sensor node is depicted in Figure 1.3. These sensor nodes are densely deployed in an area of interest to collect sensory data by collaboratively working and exchanging

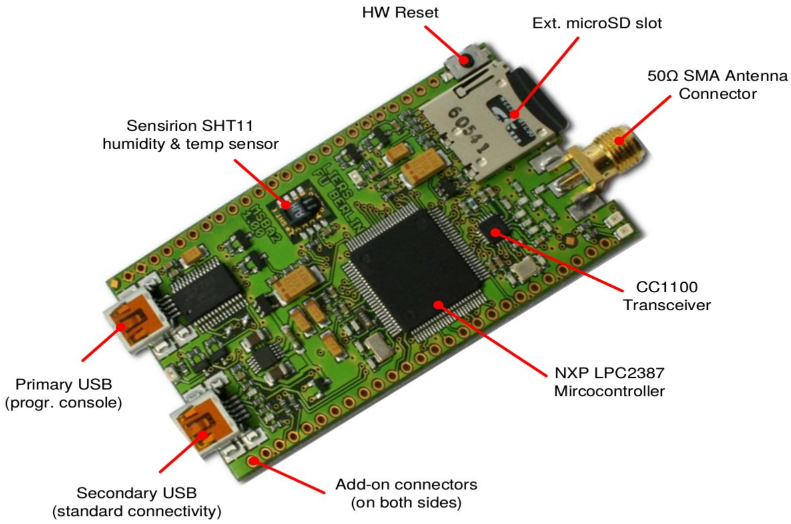


Figure 1.3: MSB-A2 sensor node [32].

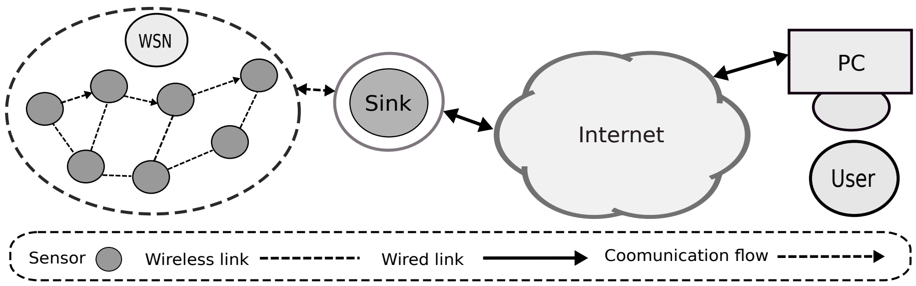


Figure 1.4: A wireless sensor network consisting of a set of sensor nodes that sense a physical phenomenon of interest such as temperature, flow or humidity and send these measurements to the sink. The sink is usually wire connected to the Internet. The arrows indicate the direction of data flow.

information wirelessly through forming ad-hoc networks as shown in Figure 1.4. Due to their ubiquitous presence and considering potential benefits leveraged by these networks such as simple deployment, cheap installation cost, no wiring cost, less complexity and mobility. They are increasingly used in industrial applications [33], which have resulted into Industrial Wireless Sensor Networks (IWSNs). WSNs can be deployed in industrial monitoring [34], process automation and control [35], emergency and safety [36] applications. In process automation and control applications certain tasks may require acting nodes known as actuators that have the capability to autonomously act on the physical environment based on sensed measurements. Over the last decade, sensors and actuators have been used together to perform autonomous tasks. The integration of industrial sensors and actuators has resulted into Industrial Wireless Sensor and Actuator Networks (IWSANs). One of the most promising applications of IWSANs is in industrial networked control systems such as closed-loop or feedback control systems. Closed-loop control systems are those that work on feedback mechanism to adjust the system [37]. They compare the actual state of the system to the desired state of the system and adjust the system as depicted in Figure 1.5.

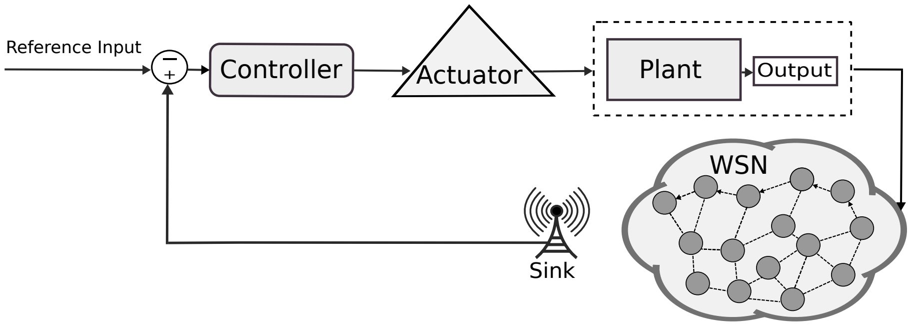


Figure 1.5: A wireless closed-loop control where the whole loop is closed through WSAN.

In a typical, feedback based chemical process automation and control, sensors measure the temperature, if temperature crosses a certain threshold value, they inform actuators (e.g., connected to a valve) to reduce temperature to a desired value so that the process remains in a stable state. Such applications impose strict constraints and requirements.

The first essential requirement is *reliable* wireless network connectivity, which is particularly important for these applications. Reliability against interference is highly indispensable because industries encompass several wireless networks, heavy machinery, and co-located communication systems that can interfere with IWSNs [38]. This can negatively impact wireless connectivity and result in link unreliability issues. Besides, most low-power wireless standards operate in the Industrial Scientific and Medical (ISM) band which can make them highly vulnerable to interference.

Second, *timeliness* or low latency are requirements that guarantee bounded and deterministic delay of data transfer between different sensors and actuators so that actions are performed on time. For example, industrial process control systems require real-time communication between machines and controllers.

Third, the network should be *adaptive* to satisfy the changing application traffic requirements. Table 1.1 shows the different classes of industrial applications, ranging from process monitoring, control, safety, and emergency operations as defined by ISA [29]. Each application category generates a different kind of data traffic. The traffic categories are listed according to traffic priority with 0 as the highest priority traffic and 5 as the lowest priority traffic.

Table 1.1: Different classes of industrial applications as defined by ISA

Category	Class	Application	Description
Safety	0	Emergency action	Always critical
Control	1	Closed-loop regulatory control	Often critical
	2	Closed-loop supervisory control	Usually non-critical
	3	Open-loop control	Human in loop
Monitoring	4	Alerting	Short-term operational consequence
	5	Logging and downloading/uploading	No immediate operational consequence

In comparison to user-generated traffic on the Internet, the traffic generated by the industrial applications has different characteristics. Most of the processes in industries are periodic in nature, meaning that they do not require frequent data transmission. The long idle periods in between data transmission makes lower power networks more suitable in comparison to traditional cellular or next generation wireless networks. Essentially, the industrial environment is heterogeneous, that is, certain traffic is an extremely high priority, while the other requires less priority. The high priority traffic requires immediate response to certain events, that is, they need the right response at the right time, otherwise, the system can run in catastrophic situations.

Fourth, network should be *scalable* enough to supporting adequate number of nodes to ensure an acceptable application performance.

Finally fifth, the *low-power operation* requirement helps nodes save power and avoid unnecessary communication attempts, thereby avoiding early death of nodes and extending network lifetime.

Such constraints induce several challenges on protocol design at different layers of the protocol stack. In particular, these requirements can be addressed through MAC sublayer which is part of the data link layer. MAC specifically administers access to shared wireless medium, avoiding collisions and managing resources. It is an important place to satisfy diverse application performance metrics like reliability, low latency, adaptivity, scalability, and energy. Therefore, exploiting characteristics of the MAC and taking a step further to employ it in IWSANs and improvise a mechanism to effectively utilize medium to achieve low latency, reliability, and energy efficiency is a compelling choice.

1.2 Contributions

We mainly emphasize on the MAC layer and evaluate existing MAC protocols so as to determine how can they meet reliable communication requirements of industrial low-power applications and propose an improved MAC protocol.

In this direction, we critically analyze existing Time-Slotted Channel Hopping (TSCH) protocol because it is considered the most reliable MAC protocol for IoT in general and the IIoT in particular. We evaluate reliability of Time-Slotted Channel Hopping (TSCH) in densely co-located TSCH networks which depicts a coexisting scenario in industries. Coexistence issue among low-power wireless networks is important because these networks share the same license-exempted ISM band. In particular, our evaluation undertakes inter-network interference problems in multiple co-located TSCH networks. We take into account clock drift of the network nodes while assessing reliability of TSCH from different perspectives such as (i) given the number of networks, analyze the ratio of successful connections and failed connections (ii) analyze the effect of diverse channels in mitigating interfering connections, and (iii) study the impact on successful and failed communications when increasing number of networks and when increasing number of nodes in each network.

Second, we study reliability of TSCH protocol under node mobility in the context of industrial low-power wireless networks as the future applications greatly demand mobile nodes to be operating in industries. We critically evaluate (i) how mobility impacts TSCH reliability in terms of synchronization, message overhead, latency, and energy, (ii) asses the impact of speed of mobile nodes on network, (iii) study network association and disassociation problems due to synchronization loss, and (iv) evaluate impact on network performance due to varying number of mobile and static nodes.

Based on our analysis, this theses proposes a Dual-Mode Time-Slotted (DMTS)-MAC protocol for industrial process control applications. Dual-Mode Time-Slotted (DMTS)-MAC is an application specific MAC that intends to guarantee application-specific performance metrics such as reliability, low latency, scalability, and energy conservation. We extensively studied existing MAC protocols that target IWSAN for control applications and carefully analyzed their limitations. Based on the identified limitations, we came up with an improved protocol that overcomes those drawbacks and offers enhanced performance. In particular, we focused on Dual-Mode Adaptive-MAC (DMA-MAC) and GinMAC protocols and enhanced the superframe structure of DMA-MAC and incorporated multichannel and channel hopping capabilities to achieve reliability, low latency, scalability, and energy efficiency.

In summary, the problem statement of this thesis primarily revolves around the following research questions:

- How does the existing communication protocols provide reliability, low latency, scalability, and energy efficiency for industrial process control applications under IWSAN?

- Can the intrinsic states of industrial process control application be exploited to make communication protocols adaptive and energy efficient?

- Is it possible to provide guarantees with respect to reliability and energy efficiency for process control applications?

- How does the coexistence of multiple co-located low-power networks impact network reliability and how does channel hopping help in this case?

- How does mobility of network nodes influence reliability of a multichannel MAC scheme and what are the trade-offs among the number of mobile nodes, speed of mobile nodes, and the number of available channels?

1.3 Thesis Organization

This dissertation comprises of total 9 chapters. The first chapter gives the reader an introduction and motivation about the topic, it also covers the background and highlights the contributions. **Chapter 2** presents background on the use of wireless technology in the context of industrial applications and highlights its benefits and challenges. It gives a comprehensive introduction and background of wireless sensor network, wireless sensor and actuator network and their applications in different industrial systems. **Chapter 3** provides a thorough discussion on the technical details of several state of the art MAC schemes taking into account their strengths and limitations with respect to industrial applications. In particular, we elaborate the IEEE 802.15.4 standard for low-power networks that supports IIoT. Essentially, we explain its PHY and MAC layer mechanisms and highlight its drawbacks. This chapter also details several low-power industrial standards such as WirelessHART, ISA100.11a, WIA-PA which target different industrial monitoring and control applications. We also raise insights on coexistence among low-power wireless networks as most of wireless standards and technologies share license exempted bands for communication which generates severe interference. Apart from industrial standards, this chapter also covers certain non-standard MAC protocols that try to address the requirements of IWSAN. At the end of the chapter, we provide a comparison of all the discussed protocols based on different metrics. The understanding of this chapter is important as this helps the reader understand the subsequent chapters presented in this dissertation.

Afterwards, **Chapter 4** describes TSCH MAC protocol which is one of the MAC modes of the latest IEEE 802.15.4 (2015) standard and it overcomes MAC limitations of its previous version (2011). We discuss the TSCH slotframe structure, network formation, synchronization, and different scheduling mechanisms. We identify certain shortcomings of TSCH based on some of the recent studies. This chapter also exposes various Internet Engineering Task Force (IETF) standardization efforts that aim to enable low-power protocol stack for emerging IIoT, this includes standards such as 6LoWPAN, 6TiSCH, and RPL. Then, **Chapter 5** presents various tools, methods, and MAC metrics used throughout this thesis. In particular, we discuss different methodologies that are used in the performance analysis of MAC protocol in low-power and lossy networks. Various simulation platforms, that we used for performance evaluation, have been thoroughly discussed along with their characteristics. We describe MAC metrics that define the criteria for many of our evaluations, and they are also commonly used in low-power and lossy networks. This chapter essentially lays the necessary base of our research methodology in this thesis.

Subsequently, from Chapter 6, we begin our contributions. In **Chapter 6**, we provide a critical analysis and evaluation on the coexistence perspective of TSCH protocol because TSCH claims to be the ideal protocol for industrial IoT. We particularly assess its reliability in dense deployment which depicts a practical use-case of the industrial applications. Our evaluation undertakes clock drifts of nodes and presents diverse experiments through simulation which provide in-depth analysis and insights on protocol behavior and interactions in different settings.

In particular, we base our evaluation from two perspectives one is the interference within the network (intra-network interference) and the other is interference due to co-location of nearby networks (inter-network interference). We take into account different aspects in the evaluation such as increasing the number of nodes in each network, increasing the number of networks, and varying the number of channels so as to determine the impact on TSCH network performance. We define connection success ratio as our preferred metric that determines successful transmission in the presence of interfering connections.

Chapter 7 undertakes the reliability test of TSCH protocol under node mobility. Our approach specifies downtime as an important metric which determines how long and how often nodes remain disassociated from the network. We asses how nodes resynchronize to the network through exchange of Keep-Alive (KA) messages and how it impacts their energy consumption. We begin our study by analyzing performance in terms of synchronization loss, speed of mobile nodes, and varying number of mobile and static nodes in restricted physical space. Apart from this, **Chapter 8** focuses on the design and evaluation of our proposed Dual-Mode Time-Slotted (DMTS)-MAC protocol that works with IWSAN for process control application. We extensively studied existing MAC protocols that target IWSAN for control applications and carefully analyzed their limitations (see Chapter 3). Based on the identified limitations, we came up with a different protocol that overcomes those drawbacks and offers enhanced performance for IWSAN. In particular, we focused on DMA-MAC and GinMAC protocols and enhanced the superframe structure of DMA-MAC and incorporated multichannel and channel hopping capabilities to achieve reliability, low latency, scalability, and energy efficiency. The evaluation are performed through simulations, for which we use OMNeT++ simulation platform which is an open source simulation environment. The results indicate the improved performance of DMTS protocol as compared to TSCH protocol under several aspects. Finally, **Chapter 9** provides an overall conclusion on the research objectives presented in this dissertation. We highlight other relevant aspects of DMTS and TSCH MAC protocols that can be taken as a part of future work to further explore in this direction.

CHAPTER 2

Industrial Wireless Sensor and Actuator Networks

THIS chapter introduces WSN, IWSN, IWSAN, and different applications that can benefit from them. During the last decade, wireless technology has been increasingly utilized in industries, leading to the Industrial Internet of Things (IIoT) mainly driven by low-power standards, which have limited range and data rate as compared to traditional WLAN and cellular technologies. IWSANs play a central role of behaving like a digital skin for the IoT. IWSANs can monitor critical parameters and control industrial processes and they can inform the industrial personnel of this information promptly. These networks have ability to offer flexibility, self-organization, rapid deployment, and low-cost operation. They have the ability to make processes autonomous, resulting in the minimal human intervention [38] when compared to their wired counterpart.

Section 2.1 highlights benefits of wireless technology in the context of industries and presents important challenges induced by it and their impact on various industrial applications. Section 2.2 discusses WSN and Section 2.3 explains characteristics of IWSN and IWSAN, and highlights difference between them. Section 2.4 describes different categories of industrial applications and talks about the requirements of IWSAN in those applications. Finally, we conclude the chapter in Section 2.5.

2.1 Wireless Technologies in Industrial Applications

Wireless technologies, despite their offered convenience, flexibility, low-cost, and mobility pose unique challenges such as fading, interference, link unreliability, and energy, which must be carefully addressed when using resource-constrained sensor nodes. The imperfect and error-prone wireless medium results in packet losses and variable communication delays. Wired networks also exhibit such losses, but in case of wireless networks, they are more amplified due to varying channel conditions, limited spectrum, interference, and fading [39]. Besides, an important issue is to efficiently utilize and provide access to the shared wireless medium, that is handled by the MAC sublayer, which is a part of the data link layer. An inefficient MAC scheme can actually waste scarce communication resources. Below we describe benefits of wireless technology and discuss important challenges induced by it.

2.1.1 Benefits

- **Cost reduction.** The main operational expenditure and capital expenditure in industries are of wiring, whose installation and maintenance incur huge costs. Using wireless solutions greatly reduces these costs. They have appealing benefits, for instance, rapid installation, easy maintenance, easy system and reconfigurations. In this way, they not only contribute to cost reduction but also save time.

- **Flexible architecture.** Wireless technologies offer a great deal of flexibility compared to wired solutions. There is no additional expenditure involved due to addition and removal of wireless sensor nodes and other necessary wireless equipment. Certain processes in industries such as the robots and the rotating equipment are severely hindered by hard and fixed locations of wired solutions, but wireless solutions can flexibly handle such processes. In addition, wired solutions are not appropriate to be deployed in dangerous areas due to surrounding temperatures, whereas wireless solutions can flexibly work in such areas [40].

- **Safe procedures.** Reconfiguration and maintenance of processes in dangerous areas are carried by humans, which can endanger their lives due to potential hazards. Wireless solutions make it safer by remotely reconfiguring and maintaining processes and systems, avoiding humans to involve in hazardous locations. Moreover, mechanical failures of connectors is a common problem in industries, which affects reliability and causes downtime of industrial applications. Wireless solutions are free from wear and tear kind of failures, which make them more safer and less prone to failures [41].

2.1.2 Challenges

- **Packet losses.** Packet losses are common in the wireless medium due to various channel impairments like interference, collisions, and weak channel gains [42]. Buffer overflow causes congestion, that renders packets to be lost in transit. Long transmission delay results in packet reordering which causes packet drop-outs.

- **Variable communication delay.** Network conditions invariably induce random delays and cause an uncertain amount of time for data to reach the destination. Data has to be sampled, encoded, and transmitted. The same has to be decoded on a receiver side which adds delay [43, 44]. For WSNs applications, the packets transmitted are timestamped which helps the receiver get an estimate of delay and take appropriate measures. For instance, under contention based MAC schemes (see Section 3.1), main causes of variability in delay arise when multiple nodes try to access same wireless link simultaneously which results in collision and then each node has to wait a random amount of time before re-accessing medium. This re-accessing the medium increases delay. Link quality between the nodes also affects delay to increase. With poor link quality, retransmissions are more frequent which increase delay as well as energy consumption. Delay is a crucial performance indicator whose variability should be as minimum as possible. An adequate upper bound for delay should be ensured so that negative impacts on application Quality of Service (QoS) can be avoided.

- **Data rate.** Limited bandwidth of the channel imposes constraint on the number of devices sharing the medium, which may impact the network capacity [43], [45]. Packet size and its overhead influence the data rate of the communication network, thus an efficient protocol may help minimize overhead. Since WSNs have low data rates, this may be a constraint for certain industrial applications.

- **Interference.** It is envisaged that the number of connected devices will grow exponentially in near future, which may cause massive interference. Most of wireless standards operate in ISM band which has left the band more crowded causing cross technology interference and self interference [46]. Although current wireless standards exploit channel diversity and time diversity techniques as in WirelessHART, ISA100.11a, and IEEE 802.15.4e to negate the effects of interference so as to promote coexistence. However, industrial environment introduces potential sources of interference such as electric motors, inverters, ignitions systems, voltage regulators, generators, frequency converters, thermal noise, friction-induced noise, and other RF signals [47]. Due to these, deep fades and channel impairments cause packet loss and link failures. Therefore, PHY and MAC layer schemes need to be well exploited to intelligently avoid such adverse effects and make the network more resilient.

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

2.2 From Wireless Sensor Network to Industrial Wireless Sensor Network

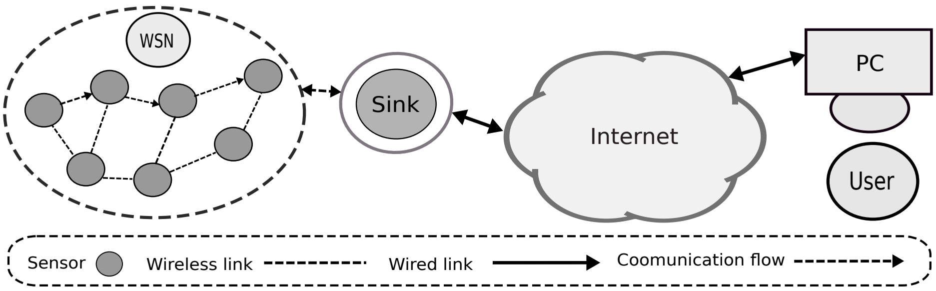


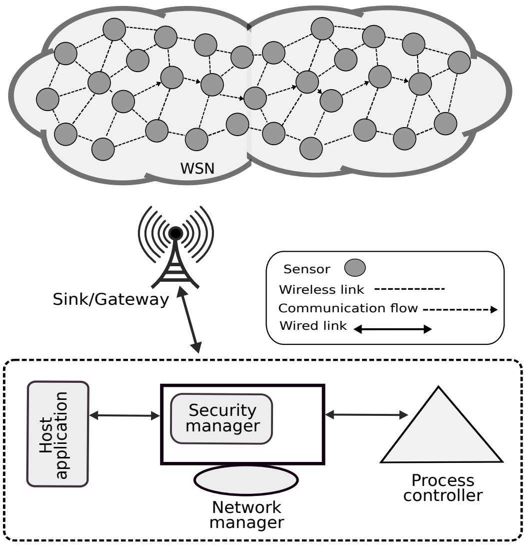
Figure 2.1: A general WSN deployment scenario.

The WSN consists of low-cost multi-functional nodes (also called motes) that along with sensing have the capabilities of processing and communication [48]. These small and low-cost sensor nodes have embedded processors and transceivers to communicate wireless over short distances. They are densely deployed in an area of interest to collect sensory data (temperature, pressure, or vibration) by collaboratively coordinating and exchanging information by forming wireless ad-hoc networks as shown in Figure 2.1. Sensor nodes are constrained in terms of power, processing, and communication owing to their small size and use of batteries. A unique feature of WSNs is their in-network processing [48] attribute, whereby sensor nodes do not send raw sensed data directly to the gateway but instead fuse it locally to make it more consequential to save extensive communication costs. Due to their unique attributes, their application domain is diverse and they are now ubiquitous components of smart environments. Their diverse application domain covers military [49], surveillance [50], home automation [51], smart city [52], and patient health monitoring [53]. In patient health-care monitoring scenarios, WSNs are used in tele-health applications [54]. For example, to monitor chronically ill patients and to regularly check their different parameters like glucose level, heartbeat and send that information wirelessly to a remotely located doctor for further diagnosis. WSNs are also used to assist elderly and disabled people in their daily routine tasks. Over the past few decades, these networks have undergone large deployments in diverse applications, including transportation [55], agriculture [56], industrial process automation and control [33, 38, 34], and supply chain management [57]. Due to their ubiquitous presence and considering potential benefits leveraged by these networks such as simple deployment, cheap installation cost, no wiring cost, less complexity, and mobility support. They are increasingly used in industrial applications [33], which have resulted into IWSNs.

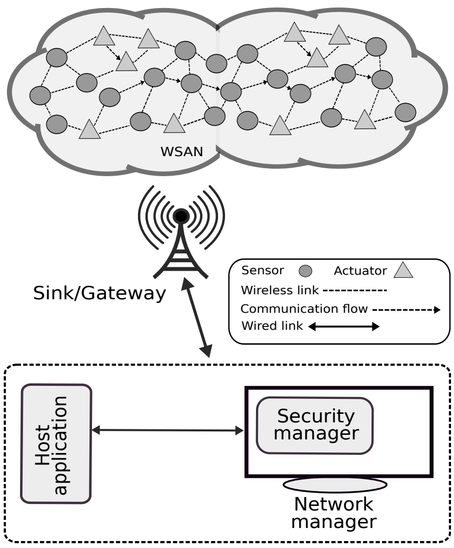
WSNs can be deployed for industrial monitoring [34], process automation and control [35], emergency and safety [36] applications. In process automation and control applications certain tasks may require acting nodes known as actuators that have the capability to autonomously act on the physical environment based on the sensed measurements. Over the last decade, sensors and actuators have been used together to perform autonomous tasks. The integration of sensors and actuators in industries has resulted into IWSANs. For example, in feedback based chemical process automation and control, sensors measure the temperature, if the temperature crosses a certain threshold value, they inform actuators (e.g., connected to a valve) to reduce temperature to a desired value so that the process remains in a stable state. Such applications impose strict constraints on reliability and low latency [58]. Because measurements of sensors have to reach the actuator timely and reliably so that the act of controlling valve is performed on time.

2.3 Industrial Wireless Sensor Network

IWSN can be considered a subset of WSN domain. Figure 2.2a depicts general architecture of IWSN that consists of WSN field, network manager-cum-security manager, process controller, and host application management. The sensor nodes in a WSN field sense the process variables (e.g, temperature or pressure) and transmit it to the sink or gateway. The sink then forwards it to the process controller whose job is to control the process variable under certain desired value. The sink is responsible to manage the sensor network and is managed and controlled by the host application management. The network-cum-security



a) General architecture of the IWSN showing sensor network field connected through the sink to controller, network manager-cum-security manager, and application console.



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

Figure 2.2: General architecture of the IWSN and IWSAN, depicting IWSN and IWSAN field together with sink. The sink is then wire connected to the rest of the industrial network (dashed line).

manager is responsible to look after the overall network along with ensuring security against attacks. The arrows in Figure 2.2a indicate the direction of the communication flow, where sensor data is transmitted to the sink in a multi-hop fashion via intermediate sensor nodes. IWSN helps to improve production processes and quality of products without compromising the quality of service.

2.3.1 Industrial Wireless Sensor and Actuator Network

Industrial process automation and control applications are increasingly utilizing WSN as part of the control operation. The increasing trend is to integrate sensors and process controller (actuators or actors) to perform sensing and actuating tasks, that is, sensor nodes have been equipped with actuators. Succinctly, the actuators are transducers that have the capability to convert an electrical signal into a physical action, a typical actuator example includes a valve that controls flow of the water or gas in a tank [59].

Actuators are also referred as actors[1] in the context of WSN, here the actors not only act on the physical environment but also possess networking capabilities such as receive, transmit, process, and relay data. For example, a robot working in the industries may act on the physical environment by means of various motors and servo-motors (actuators). However, from a networking perspective, the robot may be considered a single networking entity which we refer to as actor [60]. Thus, an actor may involve more than one actuator which means they encompass heterogeneous devices. This hybrid combination of sensors and actuators has developed a new class of research known as Wireless Sensor and Actuator Network (WSAN) [59].

Figure 2.2b shows WSAN in industries, here WSAN is a distributed sensor and actuator field where the sensors have direct communication with the actuators and the actuators can also communicate among themselves. Hence, unlike WSN, where sensors always communicate sensed data to the sink, WSAN involves sensor-to-actor and actor-to-actor data communications via single-hop or multi-hop transmissions. WSAN has the capability to perform distributed sensing, data fusion, collaboratively making decisions, and performing appropriate actions on physical environment [61]. For example, sensing water level or flow and sending data to the actuator, and actuator controls water level or flow of water. In this way, the information that is sensed can be efficiently utilized to perform appropriate actions. A distinct characteristic of actuators is that they are usually rich in resources like computational, communication, and battery power.

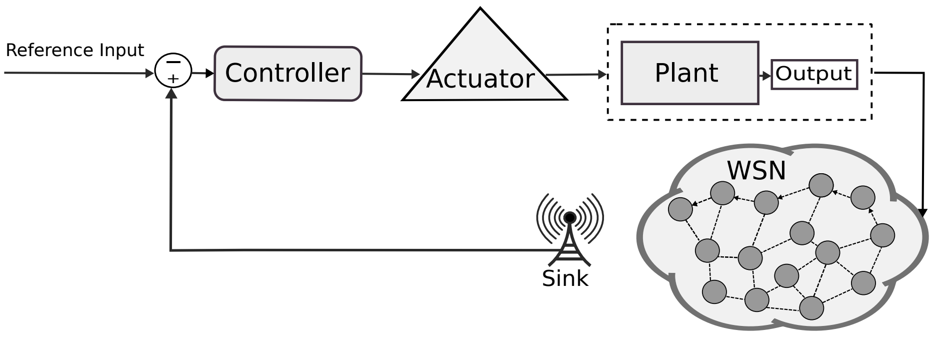


Figure 2.3: Wireless closed-loop control realized through WSN. Sensors measurements are sent to the controller through the gateway, which is wire connected to the controller.

In some cases, actuators may also perform sensing tasks. However, compared to sensor nodes, they impose strict constraints on reliability, predictability, and

[1]Throughout this text, we use the terms actuator and actor interchangeably.

availability [34, 38]. Since actuators have rich capabilities they are not as densely deployed as sensor nodes. A few actuator nodes would suffice with different coverage requirements. Additionally, the sink or gateway is required to monitor the overall network.

One of the most promising applications of IWSANs is in the industrial Networked Control Systems (NCSs) including closed-loop or feedback-based control systems. Figure 2.3 shows IWSANs in a typical industrial closed-loop control, here the whole control loop is realized through WSAN. Another interesting application of WSAN is the smart home, where based on some user prescribed settings, sensors send data to appropriate actuators to perform an action. For instance, to turn on and off light bulbs, or control air conditioning based on settings already prescribed. WSAN is a promising class of research, where not only the data is sensed and communicated but is also acted upon which is an interesting feature.

2.3.2 Characteristics of Wireless Sensor and Actuator Network

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

- **Real-time guarantee.** Real-time requirement is interchangeably dealt with latency and delay bound, that is, there are strict timing constraints involved between sensing and acting. This means that as soon as data is sensed it should timely trigger actuators to act. If the required data encounters latency and actuation command is performed late, it makes data less effective, meaning sensing data must be valid at the time of acting [61]. For example, in a fire detection and extinguishing application, once sensors sense fire, it requires timely action from actuators to trigger fire extinguishers so that fire can be controlled before it gets further deteriorated. Table 2.1 highlights the comparison between WSN and WSAN in a nutshell.

- **Reliable coordination.** An interesting feature of WSAN is that sensors not only communicate among themselves but also with actuators. Thus, there are sensors-to-actuator and actuator-to-actuator coordinations involved [61]. These coordinations involve selection of suitable actor to perform the action based on different metrics such as its available energy, coverage, distance, and location.

Table 2.1: Comparison of WSNs and WSANs in nutshell

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

These coordinations are of fundamental importance to maintain the required reliability, self-organization, and QoS of the network, but at the same time, they impose new challenges on networking to provide robust and delay tolerant protocols.

- **Traffic differentiation.** With the presence of resource-constrained sensors and resource-rich devices like actuators, the environment is heterogeneous. Therefore, efficient resource allocation and utilization techniques need to be developed. Energy efficiency for sensor nodes is a big concern but for actuators is of less concern. Moreover, actuating messages are more delay sensitive than normal sensor measurements, so message priority differs in both. Therefore, heterogeneity needs to be exploited intelligently in protocol design so that application QoS requirements and the constrained resources of sensors are not at stack.

2.4 IWSAN Applications and Requirements

Industrial domain encompasses applications, ranging from monitoring and control to safety or emergency, process automation, factory automation, closed-loop control, and predictive maintenance. Different applications require different priorities. Moreover, frequent streaming updates related to configuration changes, alarms, and command instructions keep refreshing. Based on the criticality of data, several application categories are defined by International Society of Automation (ISA), which are given in Table 2.2 (also in Table 1.1, see Section 1.1) along with their latency requirements. Next, we give a brief discussion of some of the application categories along with their traffic type.

Table 2.2: Industrial applications and their typical requirements [62, 63]

	Applications	Delay	Range (m)	Battery	Update Frequency
Interlocking and control	Proximity sensor	ms	100	> 5 years	10 - 250 ms
	Motor	ms	100	> 5 years	10 - 250 ms
	Valve	ms	100	> 5 years	10 - 250 ms
	Protection relays	ms	100	> 5 years	10 − 250 ms
Closed-loop control	Control valve	ms	100	> 5 years	10 - 500 ms
	Pressure sensor	ms	100	> 5 years	10 - 500 ms
	Temperature sensor	ms	100	> 5 years	500 ms
	Flow sensor	ms	100	> 5 years	10 - 500 ms
	Torque sensor	ms	100	> 5 years	10 - 500 ms
	Variable speed drive	ms	100	> 5 years	10 - 500 ms
Monitoring and supervision	Vibration sensor	s	100	3 years	s - days
	Pressure sensor	ms	100	3 years	1 s
	Temperature sensor	s	100	3 years	5 s
	Gas detection sensor	ms	100	3 years	1 s

2.4.1 Applications

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

- **Safety systems.** These systems are directly related to emergency actions. They are always critical in nature and require immediate action to be taken, that is, real-time communication is desired. These systems are extremely delay sensitive and require low latency and high reliability. But in terms of bandwidth requirements, they tend to have moderate bandwidth.

- **Control systems.** The major part of the industrial applications requires control operations. Several control systems exist such as closed-loop control systems [64], open-loop control systems, and process control systems. Generally, closed-loop control systems monitor processes and act accordingly as per the control decision. These systems are generally autonomous and do not involve humans in the loop. Examples of such systems include process control systems and factory automation systems. Open-loop control systems do not have feedback and require humans in the loop, that is, adjustments are done by humans. Each control system imposes different delay requirements, for example, closed-loop control data is more critical than open-loop control data.

- **Alerting systems.** These systems are characterized by the features such as regular events and alerts as a result of continuous monitoring. They indicate short-term operational consequences at different stages of processes or systems.

- **Predictive maintenance and automatic fault detection.** This is useful in industries, it ensures the prediction of a machine failure before it actually occurs [65, 66]. This is basically driven by the condition monitoring together with possible automatic maintenance utilizing advanced algorithms. This is a crucial challenge because the unexpected shutdown of machines or equipment leads to unscheduled downtime, which incurs huge losses. Therefore, a reliable sensor and actuator network is required to precisely predict the machine failure. The collaborative nature of sensor and actuator networks can jointly predict detection of faults and help avoid worst-case situations.

- **Monitoring systems.** This includes monitoring process variables, equipment condition monitoring, and structural health monitoring. The general goal of monitoring is to continuously gather data from an area of interest for long durations, analyze the data and use this data to make better decisions so as to derive certain conclusions. These systems cover almost every aspect of the industrial applications.

2.4.2 Requirements

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

- **Reliability.** The wireless medium is unreliable, link quality varies over time. It is assumed that bidirectional links do not have the same link quality in both directions. Poor link quality can deteriorate transmission and cause latency, which can deteriorate control decisions to be taken on time, which, in turn, can lead to system failures and economic losses [47]. All these factors cause unreliable links, reduced range, noisy transmission, and fading which result extensive packet loss ratio and higher packet delay. The reliability can be treated at different levels. For example, it can be a function of energy efficiency, that is, the network lifetime should be adequate enough to perform reliably over that period. Reliability can also be characterized in terms of packet reception rate, for instance packet reception rate should be above a certain threshold to guarantee a certain level of reliability in which processes and systems work without further degradation.

- **Network induced latency.** Communication latency includes processing delay, transmission delay, sampling delay, coding delay, decoding delay, medium accessing delay, and routing delay. For instance, there are three kinds of delay associated with complete cycle of control-loop process: i) delay incurred for transmission from sensors to controller T_{sc}, ii) controller processing delay T_{cd}, to compute controlling command, and iii) delay associated with transmission of controller command to actuators called T_{ca} [67]. Therefore, the total delay must be less than or equal to the upper delay as tolerated by the application. The latency should be as low as possible, often real-time guarantees are desired. Latency of tens or hundreds of milliseconds is generally considered. For example, distributed control systems in process automation have total delays ranging from 250 ms to 1 s, however samples times of as fast as 10 ms and as slower as 5 s may be found [68]. Thus, given the strict latency bounds, to achieve low latency imposes severe constraints on protocol design practices. Protocols should be designed to achieve bounded delay as required by IWSAN application.

- **Packet priority and heterogeneity.** Industrial domain is heterogeneous, different types of packets are generated like sensing measurements, controlling commands, actuation tasks [69], etc. Each of the traffic has a different priority to be treated. Therefore, adding packet priority ensures a certain degree of timely action performance. Some actions require immediate execution while others can tolerate a certain level of flexibility for execution. For example, in closed-loop control systems, controlling and actuation commands are more critical than sensor data. So a level of priority difference should be embedded in protocol design so that in case of faults system should respond appropriately.

- **Energy efficiency and power consumption.** Since for battery-powered sensor nodes, it is almost impossible to replace battery especially in inaccessible and dangerous areas in industries. Nevertheless, energy efficiency is also a major concern as reliability and latency. Improving energy efficiency also adds value to reliability in the same manner as reliability in terms of low latency and packet reception rate. However, reliability and low latency demands may cause significant energy consumption [70]. Therefore, careful trade-offs need to be taken care of under existing metrics trade-offs' complexity. Analytical or experimental evaluation to analyze the trade-offs will lead us to develop robust and flexible protocols.

- **Adaptation.** Often control applications traffic requirements change dynamically with respect to controller decisions. For example, the chemical process control applications often change states based on the data sensed by the sensors which are connected to the plant. Based on this data, the controller dynamically makes decision for changing process states and the actuators act on that decision. To cope with such a dynamic traffic behavior, communication protocol must adapt its parameters as per the requirements of control application.

- **Scalability.** Scalability refers to the ability of a system to scale well or provide a high degree of flexibility [71]. It supports adaptivity to changes with respect to addition and removal of nodes or functionality without degrading its existing performance. Generally, IWSAN may require hundreds or even thousands of nodes, therefore, communication protocols need to be scalable to comply with such requirements. However, the development of scalable MAC protocols is non-trivial task and imposes a huge challenge. Existing wireless standards such as WirtelessHART and ISA100.11a largely utilize Time Division Multiple Access (TDMA)-based protocols, which impose strict constraint on the number of participating nodes and at the same time satisfy application QoS requirements. Therefore, in order to achieve better performance, IWSANs require protocols that can support scalability at different layers of the protocol stack.

2.5 Conclusions

This chapter presented a thorough discussion on WSN, IWSN, IWSAN and addressed differences among them. It was important to highlight those differences so as to understand unique requirements due to the presence of actuator nodes. Along with this, we explained several industrial systems and their attributes with respect to criticality of traffic generated by each system. The chapter also covered discussion on wireless medium and challenges associated with it. Several requirements associated with various industrial applications were also highlighted so as to understand their peculiarities.

The next chapter deals with the state of the art MAC protocols, standards, technologies, and certain non-standard MAC protocols that target industrial monitoring and control applications.

CHAPTER 3

Prevalent MAC Schemes, Low-Power Standards, and Protocols

IN this chapter, we first present a detailed working of the MAC layer and present different categories of the state of the art MAC schemes. To this end, the efforts of research community have led to the standardization of several wireless technologies for various types of application domains depending on factors such as reliability, latency, scalability, and energy efficiency.

In Section 3.1, we discuss general characteristics of medium access control layer and how it influences communication. Section 3.2 presents the state of the art MAC schemes and their categories. In Section 3.3 and Section 3.4, we overview standard wireless technologies, we specifically study their MAC and PHY features that they proposed to address the requirements and challenges of wireless communications. Furthermore, we explain the use of these standards in various application domains, such as smart homes, smart healthcare, industrial automation, and discuss their suitability in satisfying the requirements of these applications. Various technologies and standards that share common frequency bands, such as ISM, generate severe interference in a coexisting environment are presented in Section 3.5. Here, we investigate how the inherent PHY and MAC layer design of these standards and technologies help to cope with interference issues. In Section 3.6, we provide discussion on existing non-standard MAC protocols developed for industrial process control and monitoring applications. Finally, we draw conclusions in Section 3.7.

3.1 MAC Layer Characteristics and Influence

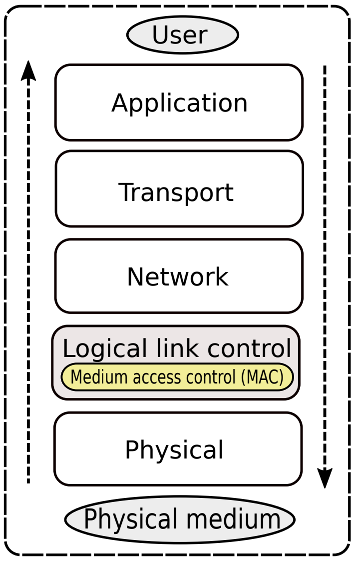


Figure 3.1: Simplified communication stack for WSN.

Due to broadcast nature of wireless medium, two nodes transmitting within their effective communication range can severely interfere with each others' transmission resulting in collisions and wastage of the resources [72]. MAC is a part of the data link layer within simplified communication stack of WSN as shown in Figure 3.1. It specifically administers access to the shared wireless medium, avoids collisions and manages resources. Depending on application requirements, it coordinates a communication schedule among nodes. MAC influences many application performance metrics such as latency, reliability, energy efficiency, and security. For example, by intelligently reducing collisions, it can control latency and energy consumption. Several MAC protocols have been developed for conventional wireless networks [73, 74], but none of them suits low-power requirements of WSNs. Because all those protocols were designed without taking into account the energy constraints of sensor nodes. Several protocols tailored to traditional WSNs [72, 75] are not suitable for WSANs, because of the coordination among sensors and actuators. Based on application classification given in Section 2.4, closed-loop control systems often require critical data delivery with low latency and high reliability. This urges to design MAC protocols that comply with these performance metrics so as to maintain the application QoS parameters.

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

3.2 State of the Art MAC Schemes

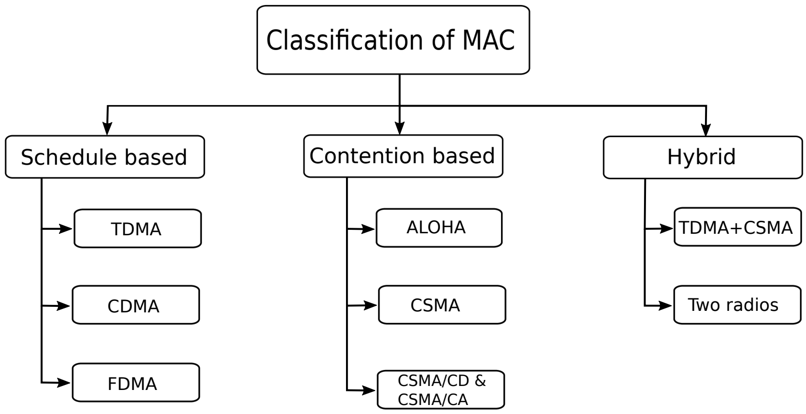


Figure 3.2: Classification of MAC protocols.

MAC protocol development has been an active area of research. A large number of MAC protocols exists in literature and can be found in [72, 75, 76]. As each application imposes different requirements for MAC, therefore, in response to fulfilling those requirements several protocols emerged. Fundamentally, each protocol, with its different design, tries to define a way to access the medium and achieve application-specific requirements. Generally, MAC schemes can be classified into three broad categories known as *schedule based, contention based* and *hybrid schemes* [77, 78] as depicted in Figure 3.2. These schemes fundamentally utilize two major multiple access approaches: Carrier Sense Multiple Access (CSMA) and Time Division Multiple Access (TDMA). Other known approaches are Code Division Multiple Access (CDMA) [79, 80, 81], Frequency Division Multiple Access (FDMA) [82], Orthogonal Frequency Division Multiple Access (OFDMA) [83], and Space Division Multiple Access (SDMA). A brief explanation of some of these categories is presented as follows.

3.2.1 Schedule based Schemes

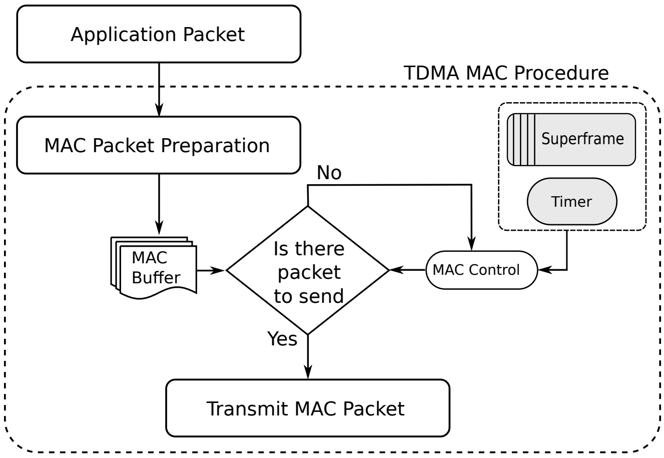


Figure 3.3: A simple TDMA MAC procedure through superframe representation.

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

- **TDMA.** Time is divided among sensor nodes and each node gets a specific portion of time, in the form of *timeslots*, to access the medium and transmit data. Most of these schemes follow a superframe structure which contains timeslots for each network node and keeps repeating for a defined duration of time. For a successful TDMA slot assignment, synchronization among nodes is crucially important. A simple TDMA scheme with a superframe is shown in Figure 3.3 [40].

- **FDMA and CDMA.** In FDMA, the available frequency spectrum is divided into a number of sub-channels. Each node is allocated a specific sub-channel. In CDMA, the signal is sent via spread spectrum technology and a special encoding scheme is used to allow multiple signals through same channel. Although FDMA and CDMA are two important medium access schemes, they are generally less suitable for WSN due to their complex design and extremely high energy consumption [77, 78].

There are several advantages of schedule based schemes like collision-free communication, inherent duty-cycle, overhearing, and idle listening avoidance [84].

All these aspects are contributing to save energy. These schemes tend to be more predictable and can offer deterministic end-to-end delay. However, with increasing number of nodes, the queuing delay is much higher because nodes have to wait for their dedicated timeslots to access medium. Synchronization is a big concern and causes high complexity in these schemes, which generate extra traffic due to control packet exchange. Generally, these schemes are less flexible and scalable, they are less suitable where dense deployment of WSN is a prime requirement.

3.2.2 Contention based Schemes

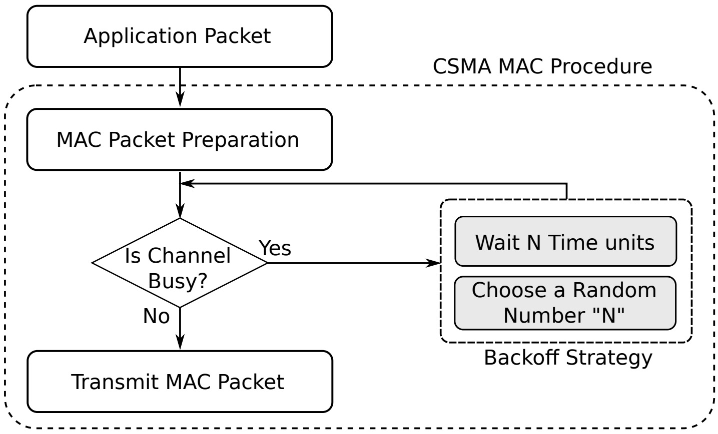


Figure 3.4: A simple CSMA MAC procedure.

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

- **Additive Link On-Line Hawaii System (ALOHA).** The pioneering protocol in this class is the ALOHA [85] protocol, in which each node initiates transmission whenever it has data regardless of the other nodes' transmission at the same time and results into collisions. Another variant of ALOHA is the slotted ALOHA which is more efficient than pure ALOHA, in which nodes initiate transmission only at the beginning of the slot which decreases the chance of collisions.

- **CSMA.** It allows nodes to be more modest in terms of accessing channel. Nodes first sense the channel to determine if any other transmission is already in progress (channel busy) if so, they have to wait a random amount of time and try again later. However, if a channel is sensed free they immediately proceed with their transmission. A simple CSMA scheme is depicted in Figure 3.4. There are different variants of CSMA scheme like *non-persistent* CSMA, *persistent* CSMA, *p-persistent* CSMA, and *I-persistent* CSMA. Each of these variants tries to minimize collisions and achieve better performance by modifying some parameters. Other variants are Carrier Sense Multiple Access/Collision Detection (CSMA/CD) and Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA).

The consequential benefits of contention based schemes are that they are adaptive towards change in network conditions and adjust their performance according to traffic loads [86]. They are more flexible to topology changes and scalable to node density compared to schedule based approach. Due to independent channel accessing decisions, they do not require extra message exchange overhead. Their main drawback is of energy inefficiency which is caused due to collisions, idle listening, and unfair load distribution. With increased node density, the probability of collisions increases which causes retransmissions and limits throughput and wastes energy. The protocols in this class can follow both centralized control and distributed control approaches similar to schedule based schemes [48, 77].

3.2.3 Hybrid Schemes

These schemes combine both schedule based and contention based approaches to offer potential improvements. They usually have two modes, one utilizing schedule based and other contention based approaches. They jointly maintain switching between the two as per the requirements. Certain examples of protocols based on hybrid scheme are Z-MAC [87], ER-MAC [88], and a Hybrid MAC protocol for WSN [89].

Table 3.1 shows the comparison among all the aforementioned MAC schemes based on different performance metrics highlighting their strengths and limitations.

3.3 Existing Low-Power Standards and Solutions

In this section, we give a detailed overview of the IEEE 802.15.4 standard which is widely known as low-power wireless standard for WSN. We also present different

Table 3.1: Different MAC schemes with their features, strengths, and limitations

Metric	Pure-ALOHA	CSMA	TDMA	FDMA
Collision Probability	✓	✓	✗	✗
Bit Rate Flexibility	✗	✗	✓	✗
Synchronization Overhead	✗	✗	✓	✓
Energy Efficiency	✗	✗	✓	✗

low-power standards based on IEEE 802.15.4. Subsequently, we discuss three industrial standards: WirelessHART [28], ISA100.11a [29], and WIA-PA [31]. The discussion mainly focuses on their PHY and MAC layers.

3.4 IEEE 802.15.4

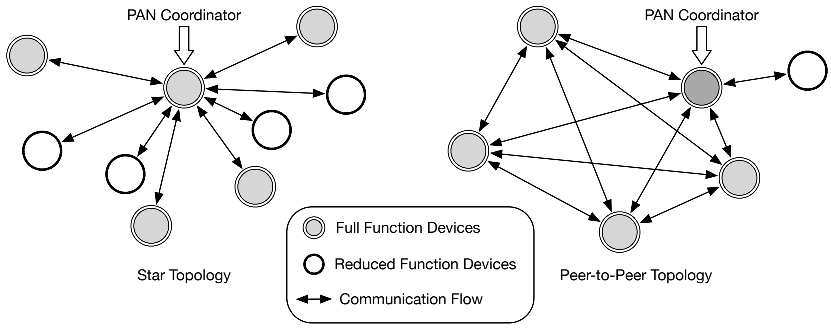


Figure 3.5: Different network topologies supported by the IEEE 802.15.4 standard.

IEEE 802.15.4 [26], which mainly defines PHY and MAC layer specifications, is considered the *de-facto* standard for low-rate WPAN. The standard was developed for low data rate monitoring and control applications that require low-power consumption. Due to its appealing features such as low-power, low-cost, and moderate data rate, it is the most widely used standard for home automation [90], industrial automation [91], smart cities [92], and wireless body area networks [93]. Most of the existing standards, such as ZigBee [27], WirelessHART [94], and ISA100.11a [29], employ IEEE 802.15.4 as the PHY layer technology together with certain upper layer modifications. At the MAC layer, the standard offers a flexible protocol that tries to achieve a better trade-off among several performance metrics, such as energy efficiency, delay, coverage, and data rate.

The IEEE 802.15.4 network supports star, tree, and peer-to-peer network topologies as shown in Figure 3.5. The network is composed of two types of devices, namely *Full Function Device* (FFD) and *Reduced Function Device* (RFD). The FFDs can perform activities like network coordination, routing, and sensing, whereas the RFDs are constrained nodes that can only serve as end-devices to perform sensing tasks. As coordinators, FFDs can form, manage, and maintain a Personal Area Network (PAN), but an FFD can manage only a single PAN at a time. The FFDs can also serve as routers that relay traffic through intermediate routes from source to destination. They can also store routing tables.

The following discussion elaborates more on the PHY and MAC layer specifications of the standard.

3.4.1 PHY Layer

The PHY layer uses the 2.4 GHz ISM frequency band. Different frequency bands are allocated to different regions, as listed in Table 3.2. The PHY offers services such as the transmission and reception of PHY Protocol Data Units (PPDUs) across the physical channel. It performs a number of suitable functionalities like

Table 3.2: Frequency bands of the IEEE 802.15.4 standard

	Europe	**America**	**Worldwide**
Frequency (MHz)	868-868.6	902-928	2400-2483.5
No. of Channels	1	10	16
Channel Bandwidth	600 kHz	2 MHz	5 MHz
Data rate	20 kbps	40 kbps	250 kbps
Modulation	BPSK	BPSK	OQPSK

the activation and deactivation of radio transceiver, Energy Detection (ED), Link Quality Indication (LQI), Clear Channel Assessment (CCA), channel frequency selection, and packet transmission and reception [26].

The purpose of the ED is to estimate the power of the received signal within the bandwidth of the channel so that the MAC layer can avoid interference.

CCA is a reliable method to determine any activity on the channel before making a transmission. CCA works based on multiple sampling of channel energy. For example, it may sample the channel five times and report a free channel if there is at least one sample less than the noise floor. There are total 27 different channels available across all of the bands as defined by the IEEE 802.15.4 standard. For example, the 2.4 GHz band includes 16 channels numbered from 11 to 25, where each channel has a bandwidth of 2 MHz and center frequencies are separated by

5 MHz. They offer an achievable data rate of as much as 250 kbps [95]. IEEE 802.15.4 uses Direct Sequence Spread Spectrum (DSSS) which mainly supports coexistence by spreading the signal over a larger bandwidth.

Upon receiving a request from the MAC sub-layer, the radio transceiver may operate in one of the three states: transmit, receive, or sleep. The energy consumption states of a transceiver can be classified into transmission, reception, and sleep states. During idle listening, the device is listening to incoming packets, which may result in overhearing packets that are not destined for it [78]. It is observed that in most of the commercial IEEE 802.15.4 compliant transceivers the energy consumed during idle listening is almost the same as receiving or transmitting a packet [96] and is a significant cause of energy waste. For example, the TI CC2420 transceiver at 0 dBm output power consumes 17.4 mA in transmission and 18.8 mA in idle listening states [97].

Since nodes have constrained resources, the IEEE 802.15.4 implements duty cycling in the MAC protocol to save power. Duty cycling allows a node to sleep by turning off its transceivers to conserve energy periodically.

3.4.2 MAC Layer

The standard proposes a flexible MAC that can mainly switch between two channel access modes known as *beacon-enabled* mode and *non-beacon-enabled* mode.

Beacon-Enabled (BE) mode

In this mode, communication is based on a superframe structure. The superframe starts with a beacon period followed by an active period and an inactive period, as shown in Figure 3.6. The active period consists of the Contention Access Period (CAP) and Contention Free Period (CFP), while the inactive period allows duty cycling. The active period is further subdivided into 16 equally spaced parts called *timeslots*. The superframe information is broadcasted through beacons at the start of the network. A beacon is a specific frame generated periodically by the PAN coordinator to update synchronization and other network related information among the nodes. A superframe is bounded by two beacons. After the beacon, the CAP immediately starts where nodes compete, using slotted CSMA/CA to transmit new packets to the coordinator or request pending packets.

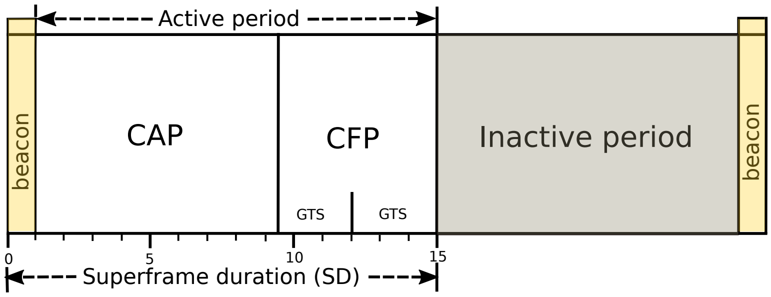


Figure 3.6: The superframe structure of the BE MAC mode of IEEE 802.15.4 standard.

A typical slotted CSMA/CA procedure is shown in Figure 3.7. To minimize the probability of collisions over the channel, slotted CSMA/CA uses the *Binary Exponential* (BE) Backoff algorithm. After the CAP is the CFP, which contains TDMA like Guaranteed Time Slots (GTSs) for transmission. GTSs are allocated by the coordinator to the nodes that require special bandwidth reservations [99]. Nodes request the GTSs from the PAN coordinator during the CAP. A GTS can be used either for transmission or reception, and a maximum of seven GTSs are allowed per superframe. During the GTS, the node has exclusive access to the channel at its disposal.

The total duration of the superframe, including active and inactive periods, can be configured through two important parameters known as *Superframe Order* (SO) and *Beacon Order* (BO). The network coordinator defines the superframe structure by a *Beacon Interval* (BI), which is the time between two sequential beacons, and a *Superframe Duration* (SD), which is the active duration of the superframe, as shown in Figure 3.6.

The values of BO and BI are related as follows [26].

$$\text{for } 0 \leq BO \leq 14$$
$$BI = \alpha \times 2^{BO} \text{ symbols}$$

α is known as $aBaseSuperframeDuration$, which is the number of symbols forming a superframe when the SO is equal to zero. The SO defines the duration of the active period including the beacon frame. The values of SO and SD are related as follows:

$$\text{for } 0 \leq SO \leq BO \leq 14$$
$$\text{SD} = \alpha \times 2^{SO} \text{ symbols}$$

Therefore, in the case of 2.4 GHz, the value of SD=15.36 $\times$ 2^{SO} ms with a BI=15.36 $\times$ 2^{BO} ms. Thus, the value of BI can be adjusted between 15 ms

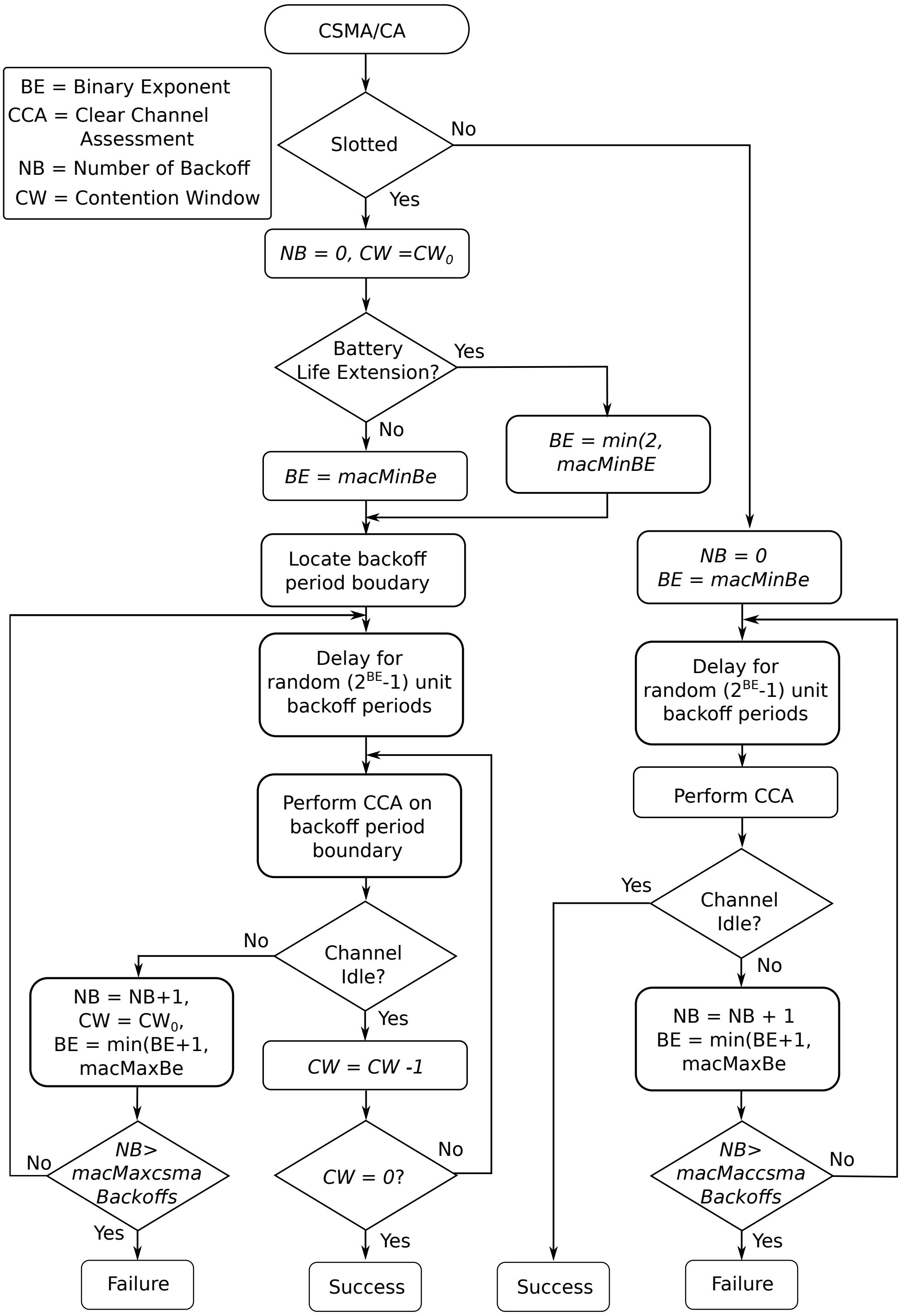


Figure 3.7: Slotted and unslotted CSMA/CA procedures [98].

to 245 s [99], depending on the value of BO and SO.

Non-Beacon-Enabled (NBE) mode

No GTS allocation is employed in this mode. Nodes mainly utilize unslotted CSMA/CA for channel access and perform only a single CCA operation without synchronization to backoff boundaries [77].

3.4.3 Limitations of IEEE 802.15.4 MAC

Although IEEE 802.15.4 MAC has several appealing features for general IoT applications, yet it has several limitations for applications that require high reliability, low latency, and energy efficiency, as pointed out in [100, 101]. To address this issue, several investigations on the performance analysis of IEEE 802.15.4 MAC were conducted [102, 103, 104, 105].

Studies in [105] show that the selection of the binary exponent is random and does not take into account the number of available nodes, the communication activity level, or the priority of data packets, resulting in a higher likelihood of collisions. The random nature of the binary exponent causes nodes to sleep for prolonged periods than required. This leaves medium unnecessarily idle for an extended period, impacting the throughput.

A simulation-based evaluation of slotted CSMA for beacon-enabled mode for dense networks was conducted in [104]. The authors showed that the backoff algorithm is not flexible for large-scale networks, since the lower limit of the backoff delay is always 0 which is fixed. Thus, it prevents particular ranges for the backoff delays. Therefore, it is not sufficient to avoid collisions for large-scale networks. The impact on the selection of the BO and SO was analyzed based on the average delay. A node that cannot complete its data transmission in the current CAP is forced to defer its transmission to the following superframe. Therefore, the node has to re-contend to access the medium and face collisions. Such a situation makes the delay for the data transmission not only non-deterministic and unbounded, but it also deteriorates the throughput.

Another study on the performance of slotted CSMA/CA for the BE mode was conducted in [102]. The authors showed that the default values of MAC parameters, such as MAC minimum binary exponent and number of backoffs, may result in lower throughput and high-power consumption. This analytical study was based on the Markov model for both saturated and unsaturated periodic traffic, and it was suggested to tune the MAC parameters to achieve better results.

Anastasi *et al.* [103] gave a comprehensive analysis on the MAC unreliability problem. The authors argued that if the power management is enabled, it will result in poor packet delivery ratio. The reason was found to be the contention access period and its default parameters, such as the minimum and maximum binary exponent value, the maximum number of backoffs, and maximum frame retries allowed. The authors suggested that the MAC, in its current form, is not suitable for mission-critical applications and requires proper tuning of the MAC parameters for better performance.

Motivated by these shortcomings, several relevant standards and protocols emerged to overcome the limitations of IEEE 802.15.4 MAC. We overview these protocols and standards as follows.

3.4.4 ZigBee

The ZigBee Alliance [27] is a group of leading companies actively working together to design and develop cost-effective, low-power, reliable wireless networking solutions for WPANs. It is the most widely used standard enabling applications across consumer, commercial, and industrial markets worldwide. It is built on top of the IEEE 802.15.4 PHY and MAC specifications but defines its own network layer. It supports star, tree, and mesh topologies. The standard can be considered as an enhancement to the IEEE 802.15.4, maintaining, supporting, and developing sophisticated protocols for residential and commercial applications. Therefore, these two standards are often confused. ZigBee provides different protocol features from network to application layer. The routing supports mesh networking along with node authentication, encryption, and security. The mesh capability has an added advantage of reliability. Nodes can also serve as intermediate relays to forward and relay traffic to destination forming a multi-hop network. This makes it suitable for large deployments. ZigBee networks can have three types of devices: ZigBee coordinator, ZigBee router, and ZigBee end devices. ZigBee coordinators are responsible to manage their own network and as well as maintain connections with other ZigBee networks. ZigBee routers are like FFDs equipped with additional functionality of routing and maintaining multi-hop communication. ZigBee end devices can act as RFDs or FFDs and they only collect and transmit the sensory information towards the router or coordinator.

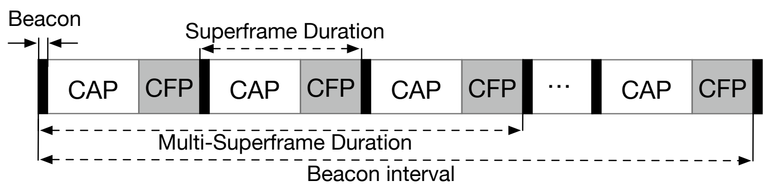
ZigBee has its own application-level framework for application layer. The application layer defines *Application Support Sub-layer* (APS) comprising *ZigBee Device Objects* (ZDOs) management and manufacturer-defined application objects [27]. The manufacturer-defined objects are used to implement applications which are based on the requirements as suggested by the standard. It supports 240 application objects. Although ZigBee has potential market share especially for home and office applications but the standard has not been adopted by the industrial applications, because it cannot provide deterministic delay and high reliability [106]. It shares the same frequency spectrum with IEEE 802.11 and Bluetooth which generate potential interference and cause MAC to frequently back off. This renders the nodes devoid of easy channel access, causing delay for the delivery of time-critical data. ZigBee does not employ any frequency-agility protection against interference and fading effects. Moreover, the static nature of the channel will create a bottleneck for ZigBee communication if other wireless LANs operate in close proximity. This also impacts delay and energy consumption because frequent packet losses will cause retransmissions, which will lead to increased delay and energy consumption. ZigBee uses IEEE 802.15.4 MAC, which renders the delay to be unbounded (see Section 3.4.3). This causes problems for real-time transmission, especially for control applications in process automation. Therefore, ZigBee has developed its variant called ZigBeePRO [107] to support industrial process and control applications.

3.4.5 IEEE 802.15.4e

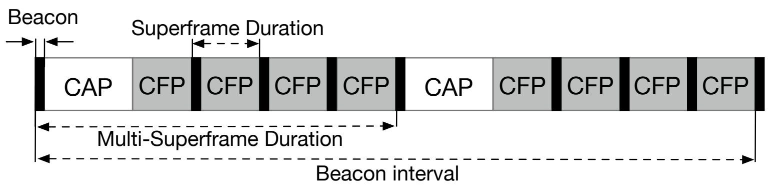
The IEEE 802.15.4 standard, in its 2011 version [26], supports enhanced physical specifications that enable a variety of applications (see Section 3.4.1). However, the standard cannot support mission-critical applications due to several limitations. Specifically, in order to meet reliability, low latency, and low-power consumption, which are the requirements of emerging applications like Cyber-Physical System based intelligent transportation system, smart health care, and industrial process automation and control, IEEE released an enhanced version known as the IEEE 802.15.4e [23]. This enhanced version specifically introduces five enhanced MAC protocols in the form of MAC behavior modes. These protocols will be elaborated in the subsequent discussion.

Deterministic and Synchronous Multi-channel Extension (DSME)

DSME is an extension of the beacon-enabled MAC mode of the IEEE 802.15.4. DSME does not rely on a single channel, instead, it uses multiple channels and has a multi-superframe structure, which has an extended number of GTSs. A multi-



a) DSME multi-superframe with extended CAP.



b) DSME multi-superframe with reduced CAP.

Figure 3.8: The multi-superframe structure of DSME MAC mode with extended and reduced CAP. The shaded bars show the CFP consisting of GTSs and the white bars show CAP.

superframe consists of a collection of consecutive non-overlapping superframes as shown in Figure 3.8.

The multi-superframe structure can flexibly support both periodic and aperiodic traffic. DSME mainly targets multi-hop networks and uses Enhanced Beacons (EBs), which are shown as black bars inside the multi-superframe in Figure 3.8. EBs are used to announce the presence of the network and contain information related to the size of timeslots, slotframe, and time synchronization information to maintain synchronization among network nodes. The superframe consists of only the active period, which is further subdivided into CAP and CFP. Nodes in the CAP use slotted CSMA/CA for channel access to transmit monitoring, urgent, or a periodic data. The CAP is fixed to 8-timeslots during which the nodes should stay awake. The CFP occupies the remaining seven slots that are known as the Guaranteed Time Slots (GTSs) (DSME-GTSs), which are used to transmit time-critical data. As mentioned before, nodes remain awake during the CAP, however, in order to save energy, DSME reduces the number of CAP periods, and only the first superframe of each multi-superframe uses the CAP. The rest of the superframes inside the multi-superframe structure do not make use of the CAP, but rather the whole period is treated as a CFP that consists of 15 GTSs, as shown in Figure 3.6 (Section 3.4.2). DSME exploits channel diversity to ensure reliability and robustness against external interference and multi-path fading.

Therefore, it is particularly suitable for factory automation, smart metering, and patient health monitoring.

DSME MAC mode is scalable due to its distributed nature. Specifically, slot allocation and beacon scheduling are not performed by a central entity, but rather they are performed by the network devices themselves in a distributed fashion. It is adaptive to time-varying traffic conditions and to changes in network topology, where each pair of nodes, based on their needs, allocates and deallocates GTS slots. Due to its adaptive capability, it can be a good candidate for mobile networks, where data rate requirements and topology vary over time. It improves energy efficiency through its *Group Acknowledgement* (GACK) option, where a single Acknowledgement (ACK) frame aggregates the acknowledgments of multiple data frames.

Although DSME MAC presents significant enhancements, some of its shortcomings have been identified as follows. For example, Rodenas-Herraiz *et al.* in [108] pointed out the overhead of topology change in large-scale networks. In particular, the overhead may be high due to the rescheduling of beacon frames and/or selection of non-interfering frequency channels, assuming the multi-superframe structure is long enough and contains superframes of all coordinators. This increases the energy expenditure of the devices. On the other hand, in a dense network, DSME incurs considerable delays due to the TDMA multi-superframe structure, where the coordinator and the devices become active only in their respective superframes. Therefore, if the part of data transmission cannot be completed in the current superframe, it needs to be deferred to the following superframe. The coordinator and its associated devices would have to wait for the next multi-superframe to resume their transmission.

Low Latency Deterministic Network (LLDN)

LLDN targets applications that require low latency, such as manufacturing and robotics. It only works with the star topology and uses TDMA superframe timeslots with small packets. The duration of the superframe is fixed and has distinctive slots, namely the beacon, management, uplink, and bidirectional timeslots. The duration of a timeslot is 10 ms, and the number of timeslots determines the number of devices that can communicate. Since the size of the superframe is restricted to a certain number of timeslots, it only allows a certain number of devices to participate in the network.

However, in order to make the network scalable up to more than 100 devices, the PAN coordinator can use multiple transceivers that each operate on a different frequency. Moreover, in order to further reduce latency, LLDN makes use of short MAC addresses to decrease frame processing and transmission time. Similar to DSME, it also exploits the GACK mechanism to minimize the bandwidth overhead. The use of star topology makes LLDN more suitable for factory automation, where a large number of nodes often communicate with a central entity. However, it has some limitations in terms of scalability, topology, and throughput.

The standard recommends using multiple transceivers in the PAN coordinator to create various networks operating on different channels. However, a study by Patti *et al.* in [109] argues that this recommendation imposes a higher cost and greater complexity. They propose multi-channel LLDN, which improves scalability by allowing a higher number of nodes in the network while maintaining low cycle times without the need of multiple transceivers for the PAN coordinator.

Berger *et al.* in [110] indicate that using a star topology restricts coverage. They propose the extension of the star topology, which is to collect data from two-hop sensors with the use of a relay node strategy. The relay nodes improve transmission reliability by retransmitting undelivered packets. The authors are of the view that the use of reserved slots and retransmission strategy in default LLDN reduces the number of sensor nodes per network, which impacts data throughput.

The Time-Slotted Channel Hopping (TSCH)

TSCH MAC [23, 111] is considered one of the latest generations of MAC protocols in the category of reliable and low-power operation. It aims to satisfy the requirements of low-power mesh networks in industrial process automation. TSCH is considered the most viable MAC candidate for the IoT protocol stack because of its time and channel diversity features [111]. It incorporates mechanisms such as *time-slotted access* and *multiple channel communication* with *channel hopping*. Time-slotted channel access inherently avoids the nodes that are competing for the channel, eliminating collisions and improving throughput. It provides every network node guaranteed access to the wireless medium, offering deterministic latency, and builds on a communication schedule that coordinates the exchange of information among the nodes. In this way, each node exactly knows when to transmit, receive, or sleep. TSCH achieves low-power through synchronization, causing the receiver to be active precisely when the sender transmits.

The improved design of TSCH is influenced by Time Synchronized Mesh Protocol

(TSMP) which is a proprietary MAC protocol designed by the Dust Networks [112]. TSMP became the widely accepted MAC protocol in the industrial domain, and in particular, is adopted by WirelessHART for its MAC operation [94]. Standards like ISA100.11a [29] and WIA-PA [31] use the core concepts of TSMP in their MAC design, alongside some higher layer packet format modifications. Please refer to Chapter 4 for complete description of TSCH protocol in detail and other emerging standards based on it.

3.4.6 WirelessHART

WirelessHART [28] is the first open wireless industrial standard, introduced by the HART (Highway Addressable Remote Transducer) [28] foundation. It is mainly designed for industrial process measurements and control applications while still being backward compatible with the HART legacy systems. It is a mesh network with self-organizing and self-healing capabilities in combination with a secure and reliable communication protocol. Although Bluetooth and ZigBee were prevalent before the release of WirelessHART, they could not fulfill the stringent requirements of industrial control applications [94]. Specifically, neither ZigBee nor Bluetooth offered guaranteed end-to-end delay and reliability.

Network Architecture

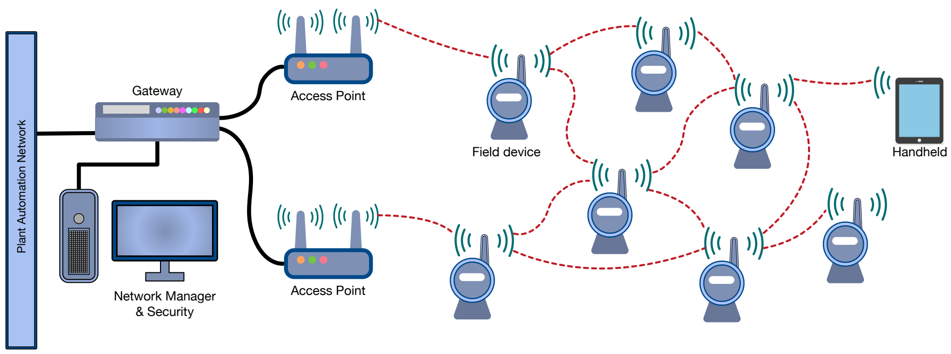


Figure 3.9: WirelessHART network architecture showing communication among different kinds of devices.

WirelessHART introduces different types of devices in the network as shown in Figure 3.9: network and security manager, gateways, access points, and field devices. The network manager is responsible for computing and maintaining the communication schedule and routing tables, as well as performing the overall network health monitoring. It can query a particular field device through the gateway as requested by the host application. The security manager and network manager work collaboratively to provide security against intrusion and attacks by generating a different session, joint, and network keys [113].

PHY and MAC Layers

The PHY layer is based on IEEE 802.15.4 [95]. TSMP is the medium access and networking protocol which offers reliable, robust, and low-power communication. It features time synchronized, dedicated time-slotted access, link layer ACKs, graph-based routing, and multi-layer security on every packet. It targets reliability of greater than 99.99% at low-power, scalability of hundreds of mesh nodes, flexibility to support time-varying traffic, security, and the ability to withstand harsh industrial environments [114]. The communication is governed by a time-slotted schedule which lets the nodes know when to transmit, receive, or sleep. TSMP follows the same scheduling scheme as of TSCH, where the schedule is computed and is represented through cells using different timeslots and channel offsets as described in Section 3.4.5.

Although WirelessHART is suitable in many aspects compared to ZigBee, it lacks public key encryption and the ability to connect to other networks without a gateway [115].

3.4.7 ISA100.11a

The standard has been developed by ISA [29] to offer secure and robust communication for industrial process automation and control applications. The PHY layer of the standard is IEEE 802.15.4 compliant and employs frequency hopping and channel blacklisting to improve robustness against interference from other coexisting networks [29].

The MAC sublayer utilizes a combination of contention based and schedule based approaches. The network layer supports IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN)[30] protocol to enable it to be connected to the Internet. The transport layer supports flow control, segmentation, reassembly, and also security. It has the ability to support both end-to-end acknowledged and unacknowledged communications [116]. Mesh and star topologies or combinations of both are supported by the standard. The ISA100.11a network comprises of sensors and actuators known as input/output (I/O) devices, which are basic field devices for sensing and actuating tasks. Routing devices ensure selection of routes towards the destination in mesh networks in multi-hop fashion and in case of primary routes failure, alternatives routes can be selected to guarantee reliability. The backbone routing device is responsible to connect to external networks by performing ISA100.11a compliant packet encapsulation. The gateway device serves as an interface between the plant network and ISA100.11a field network. The system manager performs network run time configurations, monitors communication configurations including slot allocation and scheduling. Finally, the security manager executes policies of security standard [117].

ISA100.11a MAC

The MAC takes a hybrid approach combining TDMA and CSMA/CA together with additional spatial, frequency, and time diversity to achieve real-time performance. However, in case of strict delay requirements CSMA/CA can be disabled [113]. TDMA exploits frequency hopping to enable multiple devices to

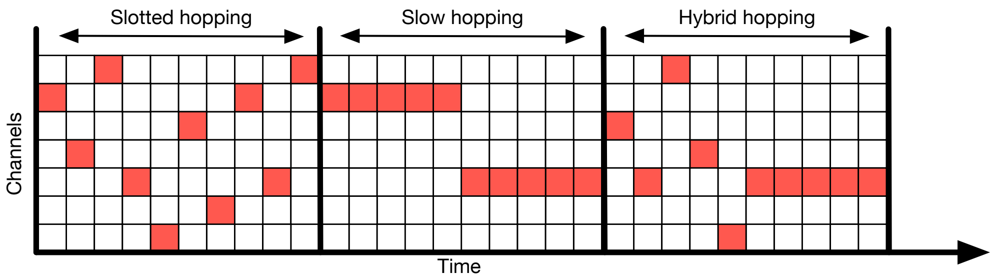


Figure 3.10: MAC with slotted and slow hopping in ISA100.11a [34, 118].

transmit simultaneously on different channels provided that only a single device may communicate on one channel per timeslot [119]. TDMA supports configurable timeslots, which means the duration of slot and superframe can be changed flexibly by modifying the two MAC parameters: *TsDur* and *SfPeriod*. Typical timeslot duration ranges from 10 ms to 12 ms [118]. Timeslot configuration employs *slotted hopping*, *slow hopping*, or *hybrid hopping* as shown in Figure 3.10. Slotted hopping enables nodes to transmit at pre-scheduled TDMA slots and the channel offset, thereby avoiding interfering channels [34]. While in slow hopping, a single channel employs a collection of successive timeslots in a period between 100 ms to 400 ms as configured by the system manager [118]. Slow hopping does not use TDMA but uses non-deterministic CSMA/CA to provide immediate channel bandwidth on demand, which supports event-based traffic in which certain events may cause the need for a device to immediately transmit an alarm or data packet. While in slotted hopping, a device is forced to wait, it is only allowed to transmit in the next scheduled slot, which causes latency to increase for event-based data transmissions [119]. Slow hopping results in more power consumption than slotted hopping since it renders the receivers to continuously listen to the channel for incoming traffic [118]. Finally, the hybrid hopping combines both the slow hopping and the slotted hopping and flexibly switches between the two.

3.4.8 WIA-PA

Wireless Networks for Industrial Automation-Process Automation (WIA-PA) [31] was introduced by the Chinese Industrial Wireless Alliance (CIWA) [120] in 2008 and is the national standard of China. It is another approved standard by the International Electrotechnical Commission (IEC) as IEC-6260 [121] in 2011 after the WirelessHART. The standard offers communication specifications and architecture for the process automation applications. It is based on the IEEE 802.15.4 standard and implements an improved version of the MAC by using three frequency hopping schemes which enable it to intelligently cope with the varying network conditions. The MAC takes a mixed approach by utilizing hybrid approach that uses contention based and reservation based mechanisms. WIA-PA network uses five types of physical devices: Host computer (user interface for management and maintenance), a gateway device (connects other networks in the plant), routing device (forwards packets through multiple device in multi-hop networks), field device (controls or monitors handheld devices), and handheld device (sensors and actuators to monitor and control the production plant) [122]. It supports combination of star and mesh network architectures in an hierarchical way, for example the routers communicate through mesh topology while the handheld devices, field devices, and routers communicate using star topology. WIA-PA recommends reactive approach to enhance further reliability and self-healing by using redundant routing and gateway devices to avoid network failures [123]. To conserve energy, WIA-PA uses two-level packet aggregation schemes natively: Data aggregation at the application layer and packet aggregation at the network layer whereas WirelessHART and ISA100.11a utilize one-level packet aggregation. It also employs security manager and network manager, the former implements and manages security keys and authentication, whereas the later configures the network, schedules communication, handles routing table, and looks after the overall network.

WIA-PA PHY and MAC Layer

The PHY is IEEE 802.15.4-2006 compliant same as the WirelessHART and ISA100.11a. The MAC is built on the beacon-enabled mode superframe structure and uses CSMA, TDMA, and FDMA approaches. Unlike the IEEE 802.15.4 standard MAC, the WIA-PA MAC implements node joining, inter-cluster management, and retransmissions during the *Contention Access Period* of the superframe [124]. Although the inactive period of the superframe is used for duty cycling to save power of the nodes, however, a part of it is also used for the intra-cluster and inter-cluster communications. It supports *Adaptive Frequency Switch*, *Adaptive Frequency Hopping*, and *Timeslot Hopping* [122] that make it highly reliable, self-organizing, and self-healing, thus, it can reliably coexist with other networks. The MAC can define frame priorities and there are four kinds of priorities highest, secondary, third, and lower priority and the schedules can be allocated based on the priorities. The synchronization at the MAC is maintained through a time source, nodes take gateways as time source in inter-cluster communication and routers in intra-cluster communication. Further, there are increasing demands to enable IPv6 datagram to be transported over WIA-PA network, one such scheme is proposed and evaluated in [123].

3.4.9 Comparison of Industrial Standards

Table 3.3 presents different wireless standards along with their PHY and MAC layer features. The comparison takes into account different performance metrics that each standard tries to satisfy.

3.5 Coexistence in 2.4 GHz Spectrum

Wireless networks are susceptible to radio interference. The impact of interference becomes even more deteriorated if they operate in the same frequency band because it causes disruptive effects in the transmission [125]. Interference can cause packet loss, latency, jitter, false alarms, and synchronization errors [125]. All of these adverse effects, in particular, cause severe problems for mission-critical applications. As the 2.4 GHz band is unlicensed globally, many technologies and standards like WirelessHART, ISA100.11a, and IEEE 802.15.4e share the same ISM band, resulting in the 2.4 GHz frequency band being more crowded. In 2003, the IEEE 802.15.2 task group [126] published standards for the coexistence of

Table 3.3: Comparison among low-power wireless standards

MAC Techniques Comparison

Feature	**WirelessHART**	**ZigBee**	**ISA100.11a**	**WIA-PA**
Physical and MAC Layer				
PHY (IEEE 802.15.4)	802.15.4-2006	802.15.4-2003	802.15.4-2006	802.15.4-2006
Data Rate	250 Kbps	250 Kbps	250 Kbps	250 Kbps
MAC Scheme	TSMP (TDMA, CSMA)	GTS, CSMA	TDMA, CSMA	TDMA, CSMA
Slot Duration	Fixed (10 ms)	Flexible	Configurable	Configurable
Frequency Hopping	Yes (Blind)	No (Frequency agility)	Yes (Blind)	Yes (Adaptive)
Network Topology	Star, Mesh	Tree, Star, Mesh	Star, Mesh	Star, Mesh
Implementation	Simple	Simple	Complex	Medium
Frame-based Priority	Yes	No	Yes	Yes
Channel Blacklisting	yes	No	Yes	No
Metric Comparison				
Reliability	✓	✗	✓	✓
Deterministic Latency	✓	✗	✓	✓
Scalability	✗	✓	✓	✓
Energy Efficiency	✓	✓	✗	✗

WPAN with other wireless networks. However, raising awareness of the new techniques and technologies do not solve the entire coexistence issue.

The problem of coexistence among BR/EDR, BLE, IEEE 802.15.4, and IEEE 802.11 networks is causing major difficulties in terms of delay and power consumption in IoT networks. Due to the massive proliferation of IEEE 802.15.4 and IEEE 802.11 networks, the possibility of interference would deteriorate application-specific QoS parameters. These networks exist in large numbers today and operate in close proximity to a number of application domains. Suitable interference avoidance solutions need to be adapted in order to maintain the required service.

As presented in Figure 3.11 the different wireless technologies operating in the 2.4 GHz band. In Figure 3.11 (a), BR/EDR is operating between 2402 MHz to 2480 MHz. It divides the frequency into 79 (1 MHz wide) channels and uses Adaptive Frequency Hopping (AFH) to avoid collisions. Figure 3.11 (b) shows BLE, which has 40 channels that are 2 MHz wide and also uses AFH. The only difference is that the advertising channels (specified with the gray color) have the responsibility of initiating the connection in connectable mode, and they are

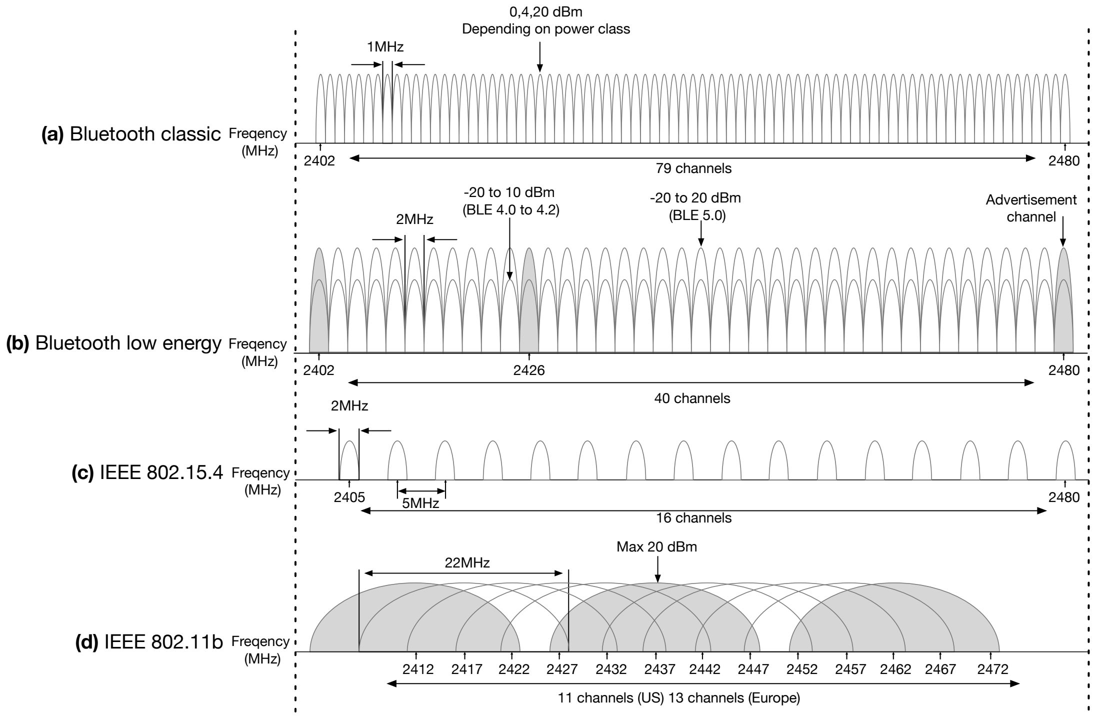


Figure 3.11: Bluetooth Basic Rate and Enhanced Data Rate (BR/EDR), Bluetooth Low Energy (BLE), IEEE 802.15.4, and IEEE 802.11 sharing 2.4 GHz frequency band.

not involved in the frequency hopping. Figure 3.11 (c) shows channel assignment for the IEEE 802.15.4 standard. Channels from 1 to 10 for the $868 - 868.6$ MHz and $902 - 928$ MHz bands are defined for lower frequency ranges, whereas the channels from 11 to 26 are operating in 2.4 GHz band. Each channel is 2 MHz wide, and the center of each channel is 5 MHz apart. Figure 3.11 (d) depicts the channel assignment of the IEEE 802.11b standard in the US. There are 11 channels, each 22 MHz wide. These channels overlap with each other, and in the best case scenario, we can only have three non-overlapping channels: channel 1, 6, and 11. However, the IEEE 802.11 standards have several versions and the channel assignment differs in some countries.

3.5.1 Coexistence of IEEE 802.15.4 and IEEE 802.11

The IEEE 802.11, more widely known as WiFi, is the ubiquitous technology defining standard for WLANs. Today, WiFi devices are everywhere, and they are causing severe interference with IEEE 802.15.4 networks. Unlike IEEE 802.15.4

devices, IEEE 802.11 devices operate at a high transmit power, high data rate, and long range. Since they are unable to sense IEEE 802.15.4 devices, they create strong interference with them. In terms of channel bandwidth, both IEEE 802.15.4 and IEEE 802.11 channels are asymmetric, that is, each IEEE 802.15.4 and IEEE 802.11 channel has bandwidth 5 MHz and 22 MHz, respectively. This causes overlapping of the four IEEE 802.15.4 channels, as shown in Figure 3.11. In most cases, IEEE 802.15.4 is vulnerable to interference [127], however, in certain cases, it does cause interference [128].

In order to improve network performance and support coexistence, these technologies inherently utilize specific techniques that help to promote coexistence. For example, IEEE 802.15.4 employs a number of inherent mechanisms such as DSSS, CSMA/CA, CCA, low transmit power, low duty cycle, channel alignment, ED, and LQI as explained in Section 3.4.1. DSSS promotes coexistence and protects against interference by spreading the signal to a wider frequency through chipping code. Chipping code is achieved by mapping the bit pattern of the signal into a higher data rate bit sequence. As the signal is spread over a larger bandwidth, the narrowband interferer blocks a small overall percentage of the signal. The receiver is able to easily recover the signal [129]. CSMA/CA works on a "listen before talk" principle, where the transmitting devices PHY continuously samples the channel and notifies the receiving device when it is clear to transmit. In this way, it is less likely to cause collision and interference with other signals. The radio turnaround time for IEEE 802.15.4 is 192 µs, while the turnaround time of the DIFS (Distributed Interframe Space) of IEEE 802.11 is 50 µs. This can cause IEEE 802.11 devices to easily preempt the channel access while the IEEE 802.15.4 device is still in the process of radio state switching. Acknowledged transmission and retries further ensure reliability, where the receiver acknowledges a successful data reception. If the receiver does not send an ACK in a stipulated time, the sender assumes failure and retransmits data by using its retry limit. This can be particularly useful when the IEEE 802.15.4 device is encountering interference when coexisting with Bluetooth. Bluetooth may interfere with the first transmission, but then it would hop to another channel. A retry helps the IEEE 802.15.4 device to make a successful transmission on the second attempt. However, studies in [130] show that the timing mechanism employed in CCA mechanism of IEEE 802.15.4 is much longer than that of IEEE 802.11 b/g, and it causes IEEE 802.15.4 to be in an adverse situation in terms of channel access competition.

IEEE 802.15.4e TSCH mode [23] uses channel hopping to promote coexistence.

Every transmission happens on a different channel. This helps to further counter the effects of interference from other co-located networks. Likewise, WirelessHART utilizes channel hopping in combination with channel blacklisting to deal with interference effectively. With this method, a channel that is continuously causing transmission problems is eliminated from the list of available channels. ISA100.11a employs AFH using slow hopping, fast hopping, and a hybrid combination of both.

Although these techniques avoid interference to some extent, the rising penetration of these networks in different domains prompts the need for more advanced and sound interference avoidance techniques in order to help these technologies coexist constructively. Especially for mission critical industrial applications, the issue of interference in a coexisting environment becomes more challenging due to the real-time characteristics of these applications which always require bounded latency and high throughput.

The issue of coexistence between IEEE 802.15.4 and IEEE 802.11a/b/g has been discussed in [130, 127, 128]. For instance, in [130], it is shown how severely an IEEE 802.11 network can interfere with an IEEE 802.15.4 network and degrade its performance. This performance degradation can lead to adverse consequences for application QoS requirements. For example, consider a fire detection application based on IEEE 802.15.4. If there is a substantial packet loss due to massive IEEE 802.11 interference, the fire extinguisher may not trigger within the set latency bounds, leading to catastrophic consequences. Angrisani *et al.* [125] experimentally studied the coexistence of ZigBee and WLAN. The experiment was conducted by varying different characteristics, such as packet size, packet rate, and SINR, under different topologies. The authors confirmed that ZigBee and WLAN could coexist but to the detriment of packet loss rate and throughput. Guo *et al.* [131] conducted experimental tests to assess the interference from an IEEE 802.11 transmitter, Bluetooth transmitter, and microwave ovens sources on the link reliability of IEEE 802.15.4 devices. Through their results, the authors show that these interference sources cause significant packet error rate. The value of packet error rate varies from 2% with no interference sources to an upward 25% depending upon the distance between receiver, transmitter, and interference sources.

3.5.2 Other Sources of Interference

Microwave ovens use electromagnetic waves in the 2.4 GHz band. Although they are covered by a Faraday cage, there is still some leakage that occurs around the doors. These waves increase the motion in water molecules and heat up food [132]. According to the US Department of Energy (DOE), more than 90% of houses have microwave ovens [133]. They also share the same spectrum and cause interference for networking devices based on WLAN, Bluetooth, and IEEE 802.15.4. Microwave ovens normally generate 60 dBm signal power and operate in a different range in 2.4 GHz (model dependent). Results show that the radiation from microwave ovens that operate in the vicinity of WSN networks can cause up to 92% packet loss [134] in WSN. This increases further interference for wireless networking devices in the 2.4 GHz band. In [130], the authors investigated the coexistence of WLAN and ZigBee networks in the presence of microwave ovens. The experimental results show that the microwave oven is a dominant interferer and it significantly increases ZigBee's packet error rate. In [135], the authors analyzed the characteristics of microwave ovens and their effect on BR/EDR. The experimental results show that the AFH mechanism enables BR/EDR to be able to tolerate a high level of interference at a distance of one meter.

Cordless phones are available almost everywhere. Most of them operate in the 2.4 GHz band like microwave ovens. They use DSSS or Frequency Hopping Spread Spectrum (FHSS) to overcome interference and achieve better voice quality. Generally, the DSSS method changes the channel manually, while the FHSS method automatically changes the channel. Similar to microwave ovens, the frequency range and the technique used in these devices are model dependent, and there is no global standard for them.

3.6 MAC Protocols for Time-critical Data Delivery

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

3.6.1 GinMAC

Suriyachai *et al.* proposed GinMAC [76], a TDMA-based MAC protocol for the largest European project named GINSENG [35]. The deployment of the project was carried out in the largest oil refinery plant located at Sines, Portugal. GINSENG offers a solution to implement performance control for closed-loop control applications using WSN. The protocol is designed to support reliable and timely data delivery in industrial process automation. It aims to meet requirements of bounded delay from the sensor to the sink as well as from sink to actuators. It is based on the tree topology and comprises of the following unique attributes like *off-line dimensioning process*, *exclusive* TDMA, and *delay conform reliability control*.

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

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

3.6.2 PriorityMAC

Shen *et al.* proposed PriorityMAC protocol in [136] for critical traffic in IWSAN. It is a priority enhanced MAC protocol and provides service differentiation for traffic categories of different priorities. The priority mechanism enables high priority traffic to hijack the transmission bandwidth of low priority traffic [136]. It considers three kinds of traffic categories according to priority like safety, control, and monitoring. Among them safety is the most critical, then control, and finally monitoring. The traffic needs to be transmitted with low latency and high reliability according to its priority. The critical traffic is prioritized over non-critical traffic in order to avoid system instability and losses, because the unpredictability regarding the arrival of critical traffic (aperiodic traffic) creates difficulties with regard to making a suitable scheduling or reserving the wireless bandwidth. It employs WirelssHART and ISA100.11a as a baseline and offers a MAC mechanism to improve access for critical traffic. The experimental evaluation shows a reduction of 94% latency for high priority traffic and 93% for secondary priority traffic on average. The experiment was conducted through TinyOS on TelsoB motes. The working principle of the protocol is that it employs four distinct access methods (AM) concurrently operating within the protocol and meeting requirements of different traffic categories (TC). Each of the TC conforms to one AM. There are four traffic categories denoted as TC1, TC2, TC3, and TC4. Each of them uses its corresponding AM for medium access. TC1 has the highest priority over TC2 and then TC3 and TC4. TC3 and TC4 utilize TDMA and TC2 uses joint backoff and indication approach. When there is a TC2 packet that has to be transmitted, it starts a backoff process. During backoff, it sends a jamming indication to defer the attempts of TC3 and TC4, meanwhile it also takes care of the same or the high priority traffic by listening to the medium so that any possible collisions can be avoided. TC1 having the highest priority persistently sends jamming indication until the channel is found idle after that, it begins transmission. The design strategy is that the PriorityMAC can hijack timeslots of low priority traffic by deferring and even destroying its attempt and transmission. There is a set of access methods for PriorityMAC and High Priority Indication Space (HPIS) associated with AM to differentiate the channel access. TDMA access mechanism within the protocol works by an algorithm which utilizes timeslot series known as superframe duration to allocate bandwidth to each communication link. Thereby allowing each link to get a periodic chance to utilize its dedicated slots to transmit its packets. A slot is then further divided into a series of subslots considered as minimum time unit. HPIS is introduced and is composed of two subslots. HPIS is inserted between the end of a slot and the start of next slot. It allows high-priority traffic while deferring the lower priority traffic, alongside it also avoids collisions with same or high priority traffic. Although the protocol provides packet differentiation but the design complexity is very high. Moreover, the access delay of high priority traffic is non-deterministic.

3.6.3 QoS-MAC

Suriyachai *et al.* proposed a QoS-aware MAC protocol in [137], which aims to provide predictable end-to-end message transfer delay and reliability. Authors define a collision-free TDMA schedule by employing fixed length time portion known as epochs. A node having no data to transmit in its reserved epoch simply transmits a control signal to its parent indicating no transmission. Cross-layer approach is employed by embedding routing at MAC. Topology awareness is built in the MAC layer to ensure deterministic end-to-end transport performance. Each node follows a different duty cycle to save energy depending on its position in a pre-determined tree topology. Retransmission slots are reserved to cope with the wireless errors and consume extra energy. Although the design aspects of the protocol match the IWSN application classes that require different QoS guarantees, however, synchronization problems can occur frequently due to clock drifts in child-parent sensor nodes. Proper slot assignment and duty cycling require each nodes to determine their position in the tree which causes the protocol not to scale well for large networks.

3.6.4 WirArb

Wireless arbitration (WirArb) is priority enhanced MAC protocol [138] targeting IWSAN applications. It is based on different arbitration frequency levels which gives an ordered channel access to each network device. In this way, nodes with highest priority gain immediate access to the medium and thus achieve real-time performance for time-critical traffic. Zheng *et al.* consider TDMA to be less suitable for safety systems in industries because these systems need immediate response to trigger and cannot wait for their dedicated TDMA slots to proceed with their transmission.

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

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

3.6.5 Breath

In [139], Park *et al.* suggested Breath: An adaptive protocol for industrial control applications for reliable and timely data transmission while minimizing energy consumption. The protocol is a simple cross layer protocol based on randomized routing, CSMA/CA MAC, and duty cycling. The basic design scheme depends on a constrained optimization problem where the objective function is the energy consumption and the constraints are the reliability and delay. The authors give a clear analytical relation among reliability, delay, and energy consumption as a function of MAC, routing, and duty cycle. They systemically verify their approach based on sound approximations. An adaptive algorithm is proposed which dynamically adapts to the network traffic and channel conditions as per the application requirements. A feedback based control loop scenario is considered consisting of plant, sensors, and controller. The goal is to remotely control the plant over a multi-hop WSN. Multi-hop capability is achieved through cluster based topology with *h-1* relay clusters. A data packet reaches the sink through relay clusters taking a multi-hop route. Breath uses randomized routing instead of fixed routing approaches because it offers flexibility for mobile equipments and reconfiguration for control applications. On the other hand, fixed routing schemes impose considerable overhead of maintaining routing tables.

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

3.6.6 DMA-MAC

Kumar *et al.* proposed Dual-Mode Adaptive-MAC (DMA-MAC) protocol in [140], which is specifically designed to support feedback based process control applications for IWSAN. It is based on TDMA superframe structure and mainly focuses on two operational states of feedback based process control namely: *transient state* and *steady state*. The protocol meets varying traffic requirements of both operational states of the control hence dual-mode (having two modes). The design of the protocol is mainly influenced by the GinMAC protocol with some changes to support two operational modes. Its aims to support key performance metrics such as reliability, predictability, throughput, low delay, and energy efficiency. The protocol switches between two operating modes and the act of switching is a critical procedure. Switching takes place based on a pre-defined threshold breach observed by the sensor nodes. The transient to steady state mode switch is performed on the basis of preset characteristics, whereas the steady to transient state switch is observed and notified by the sensor nodes to the sink. Due to its dual-mode ability, it handles large traffic loads of transient state and switches back to the steady state adaptively to support low traffic loads and conserves energy. It has two separate superframes, one for the transient state and the other for the steady state. The protocol considers the network manager as an integral part of the overall network solution and can be used as a part of the wireless standards like WirelessHART and ISA100.11a. The superframe has notification slots for state switch notifications, sensors slots to transmit the sensor measurements to the sink, retransmission slots to enhance the reliability, controller slot to process control decision, actuators slots to receive commands from the controller via the sink, alert slots to alert the sink to switch for the operational modes, and sleep slots to conserve energy. Although the protocol takes into account the process dynamics and service differentiation, yet it has some limitations for scalability. It is limited to only 25 nodes and does not scale well due to TDMA usage and strict delay requirements. Due to dual-mode nature, the protocol has a complex protocol design resulting in a large code space which affects the hardware.

3.6.7 Comparison of MAC Protocols

Table 3.4 gives the comparison of the all the aforementioned protocols. This comparison is based on different performance metrics that each protocol targets to improve. Although all these MAC protocols try to satisfy the stringent requirements of IWSAN applications, however, they do not fully conform to all the performance metrics. Therefore, more research is needed to developing MAC schemes. The goal is to overcome the existing challenges and focus on future research directions while proposing new protocols that can help realize the smart industry initiatives.

Table 3.4: Comparison of MAC protocols based on different performance metrics

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

3.7 Conclusions

This chapter looked at many state of the art MAC schemes, wireless technologies, and standards. We focused on the PHY and MAC layers because they directly influence many of the performance metrics. In our attempt to explore suitability of these standards in different applications, we highlighted several drawbacks of the MAC protocols of those standards. We also discussed interference issue among the coexisting, low-power wireless networks, which is a major challenge that degrades the network performance for reliability and latency. We analyzed how the inherent schemes employed by the standards cope with the interference issues. Certain non-standard MAC protocols that target industrial applications were also studied.

CHAPTER 4

Time-Slotted Channel Hopping MAC

THIS chapter provides technical details of TSCH protocol. We describe characteristics of Low-Power and Lossy Networks (LLNs) and give a brief discussion on different standardization efforts pertaining to TSCH that support link scheduling, routing, and IPv6 in low-power networks.

In Section 4.1, we describe TSCH protocol and its working mechanism including its slotframe structure, network formation, synchronization, and scheduling. In Section 4.2, we discuss 6LoWPAN, a routing protocol adaptation widely used in low-power and lossy networks. Section 4.3 discusses IPv6 Over TSCH (6TiSCH) protocol stack. We discuss IPv6 Routing Protocol for Low-Power and Lossy Networks (RPL), a routing protocol for low-power lossy networks, in Section 4.4. Finally, we conclude the chapter in Section 4.5.

4.1 Time-Slotted Channel Hopping

TSCH plays a central role of medium access functionality for many of industrial standards, such as WirelessHART and ISA100.11a, to meet the strict reliability, deterministic latency, and low-power consumption aspects of industrial applications. The earlier MAC protocol of IEEE 802.15.4 (see Section 3.4.2) used a single channel approach in combination with the backoff algorithm to avoid collisions in a shared medium. TSCH takes a multi-channel approach by utilizing channel hopping and maintaining a low duty cycle which outperforms single channel communications. Channel hopping intelligently reduces the impact of external interference and multi-path fading [141], which makes TSCH highly reliable and robust. Today, TSCH commercial products offer 99.9% end-to-end reliability while consuming an average current that is below 50 µA at 3.6 V [142].

4.1.1 TSCH Slotframe

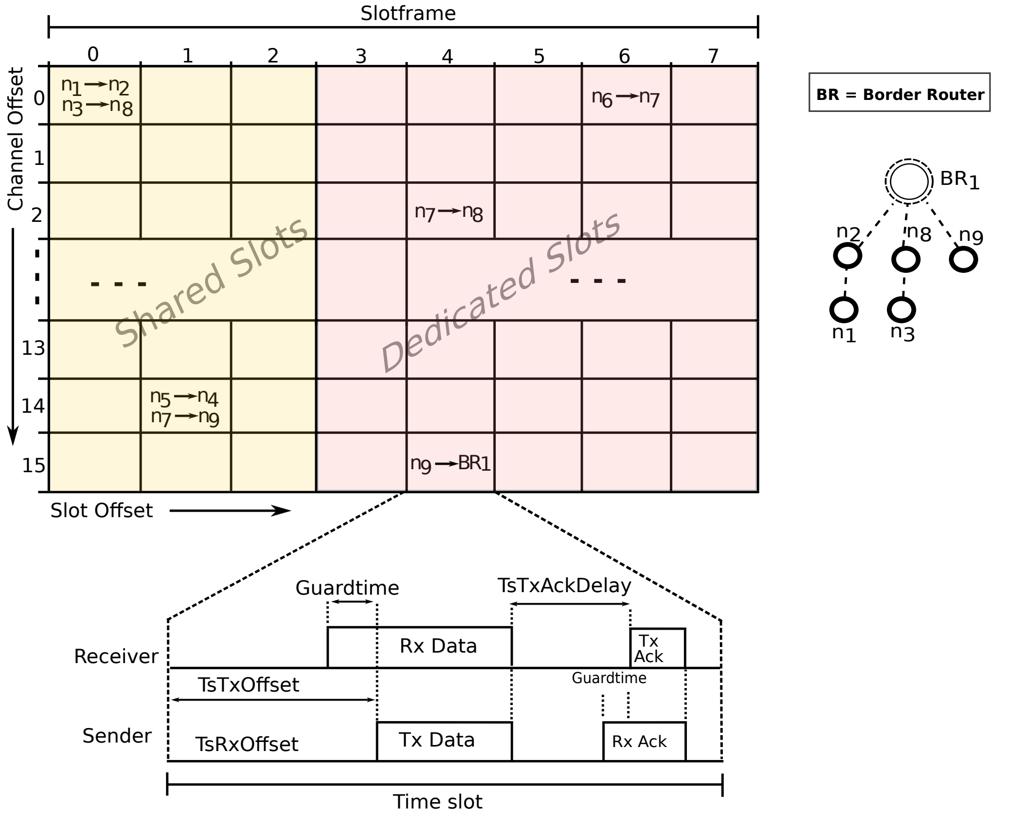


Figure 4.1: (a) TSCH slotframe showing dedicated and shared slots for the associated topology in (b). It also depicts typical sequence of events taking place within a slot between a sender and a receiver.

TSCH works on a slotframe structure, which enables all the nodes to synchronize and communicate. A slotframe combines several timeslots that repeats periodically and it can be seen an scheduling matrix as denoted in Figure 4.1. Not only does this periodic repetition of slotframe provide each node the opportunity to communicate in the network, but it also helps update synchronization and other network related information. TSCH does not define and impose a slotframe size; instead, the slotframe size is a design parameter that is decided by the application programmer. Typically, the size of slotframe can range from 10's to 1000's timeslots long [143]. A shorter slotframe offers the frequent repetition of slotframe giving the nodes frequent opportunity to transmit. Thus, results in more available bandwidth but at the expense of more power consumption of node. A possible slotframe-based communication schedule is depicted in Figure 4.1. The slotframe is eight slots long, and there are sixteen channel offsets available. Each communication link in the slotframe matrix can be assigned a cell. Each node only cares about the cell it is allocated. For example, in Figure 4.1, when node n_7 transmits a packet to node n_8, it uses timeslot 4 from the dedicated timeslots and channel offset ($Ch.2$). A frequency for a given cell can be computed through equation (4.1).

$$frequency = F\Big[\Big(CO + ASN\Big) \mod nFreq\Big] \tag{4.1}$$

Where *Absolute Slot Number* (ASN) acts as a timeslot counter shared by all the devices, which keeps track of the amount of timeslots passed since the creation of network. CO is channel offset, F contains the set of available channels, $nFreq$ is the size of F. Channel offsets can be as many as there are available frequencies, even if the two nodes have the same channel offset, but a different ASN will translate into a different frequency. ASN can be calculated with the equation 4.2.

$$ASN = (k * S + t) \tag{4.2}$$

Where k defines the repetition of slotframes since the network was started, S is the size of the slotframe, and t is slotOffset. ASN is initialized to 0 at the start of the network and is incremented globally in the network at every timeslot [23].

A slotframe can define dedicated timeslots as well as shared timeslots. Dedicated slots are contention-free which means that only a single sender-receiver node pair is allowed to communicate. Whereas the shared slots are contention-based where multiple sender-receiver node pairs are allowed to communicate and these slots are usually used for broadcast or signaling communication. As shown in Figure 4.1, a common practice is to locate shared slots at the beginning of the slotframe. For example, nodes n_1 and n_3 share a slot at channelOffset 0 and slotOffset 0 to forward their traffic to n_2 and n_8 respectively. It is possible that shared slots can encounter repeated collisions for which the standard defines a CSMA/CA mechanism to coordinate concurrent transmissions to reduce collision probability.

A timeslot is long enough to send a maximum size packet and receive its corresponding ACK. If an ACK is not received in a defined time period, the retransmission will follow the subsequent timeslot that is scheduled for the same (transmitter-receiver) pair of nodes. The guardtime, denoted in Figure 4.1, is introduced to ensure the packet be received completely. Generally, under the IEEE 802.15.4 compliant radios, transmission of a maximum size frame with MAC payload of 127 bytes takes 4.256 ms and the ACK takes around 1 ms time [111]. The default duration of TSCH timeslot is suggested to be 10 ms, which means around 5 ms time is used for packet transmission and the remaining 5 ms time can be used for other operations related to radio turnaround, packet processing, and security.

4.1.2 TSCH Channel Hopping Mechanism

As IEEE 802.15.4 contains 16 channels for communication at 2.4 GHz. Therefore, TSCH MAC implements channel hopping which enables nodes to switch channels periodically with the aid of a channel sequence known to both sender and receiver. In this way, each transmission may happen on a different channel which achieves resiliency against fading and interference. In addition, the use of parallel slotframes is also supported by TSCH, where a node can participate in multiple slotframes. Each slotframe executes a different schedule based on the application metrics and constraints. This gives the possibility to meet different QoS requirements of various applications in multiple slotframes.

4.1.3 TSCH Schedule

While the IEEE 802.15.4e for TSCH MAC, explains how to execute a communication schedule but how such a schedule is constructed and maintained is out of the scope of the standard. The schedule must be designed carefully so that when a sender transmits to a receiver, the receiver should be listening on the scheduled timeslot and channel. The scheduling rules seems intuitive though, but they emphasize the fact that the schedule be carefully allocated and be constantly refreshed as the communication links tend to be unstable and unreliable [144]. Therefore, schedule may allocate additional retransmission opportunities to cope with transmission failures. Depending on application, scheduling can be managed in different ways such as centralized or distributed.

Centralized Scheduling

In this approach, a particular network manager, a PAN coordinator or *Path Computation Entity* (PCE) is responsible to build and adjust the communication schedule of network according to network state and traffic requirements of nodes. Nodes regularly update network manager about the presence of its neighbor nodes and the amount of data it generates. Based on this information, network manager forms network radio connectivity graph, assigns timeslots and channels in schedule. After the schedule is built, it informs all nodes and each node follows that schedule.

In case, a node looses connection to its neighbor and informs manager, manager updates its schedule and informs the node. Centralized scheduling is key to make wireless deterministic as the manager exactly knows the requirements (e.g. traffic, delay) of network nodes. Most of the IWSN prefer centralized way of scheduling which is managed by the network manager that has the global view of the overall network.

Distributed Scheduling

In this approach, nodes locally negotiate with their neighbors (node at a maximum hop or euclidean distance) to construct the schedule as to which timeslot and channel to use. The negotiation involves delay or bandwidth requirements and the adherence to certain constraints to be met by the application. The nodes may adapt the schedule based on the changes in application traffic requirements or change in topology. This approach is suitable for highly dynamic networks where the topology of the network is constantly changing such as mobile network. However, it does not guarantee deterministic behavior and incurs high energy consumption of nodes due to exchange of additional signaling message overhead.

TSCH Minimal Schedule

TSCH minimal schedule comprises of a single slotframe having tunable slotframe size. The size of the slotframe is announced in EB. Only one timeslot is scheduled per slotframe, timeslot can be scheduled at any slotOffset and channelOffset and the remaining timeslots are unscheduled [145]. The scheduled slot is a common shared slot which can be used to transmit or receive link layer frames, unicast frames, and broadcast EBs [146]. Minimal TSCH schedule aims to provide interoperability, flexibility, and fallback functionality during network failure for the time when no other schedule is present [147]. The schedule is generally preconfigured into nodes or it is learned by nodes during network joining process.

4.1.4 Network Advertising and Formation

The presence of TSCH network is advertised by the nodes through the transmission of EBs. An EB is a frame that contains information related to channel hopping, synchronization of timeslots, slotframe size, and the TSCH network in general. One of this information is the *join-priority* as defined by the standard [23]. Nodes looking to join the network continuously listen for EBs from other nodes and associate with network upon successful reception. When receiving several EBs, the preferred TSCH parent is chosen according to the join priority value. Capturing beacons is complex in TSCH networks due to channel hopping because nodes are not aware of the hopping pattern prior to joining the network. Therefore, they keep switching channel every fixed duration of time until an EB is received.

4.1.5 Synchronization

Synchronization of clocks is fundamental requirement for TSCH to sustain a reliable communication in a slotframe-based network. All nodes must be equipped with clocks to keep track of time. In a typical TSCH personal area network, time propagates outward from the PAN coordinator [23]. Each node periodically synchronizes its clock with at least one other network node which is known as time source neighbor. However, as time passes clocks in different nodes encounter drifts which causes nodes to desynchronize from one another, thus each node needs to resynchronize to its time source neighbor periodically. TSCH requires clock synchronization accuracy in microseconds. Usually, the PAN coordinator or a Border Router (BR) is the source of the clock synchronization for all the nodes and it initiates EB emission. In case the network does not have any PAN coordinator, the time-source is chosen as defined by the standard. Nodes in a TSCH network can disassociate from the network due to synchronization issues and thus need to resynchronize to their time-source. Such resynchronization takes place in two different ways: 1. *frame-based* 2. *acknowledgement (ACK)-based*. In the former, node upon successful reception of the frame adjusts its clock internally by comparing the frame reception time against the expected time. Whereas in the latter, the receiving node calculates the delta between the frame reception time against the frame expected time and embeds this information in the ACK back to the sender. Apart from this implicit synchronization during data exchange, TSCH also defines an additional way to maintain one-hop synchronization in the network which is based on the exchange of Keep-Alive (KA) messages [148]. KA messages are exchanged when node has not communicated to its neighbor for sometime because of having no traffic in the network and it is no more synchronized. Thus, node can exchange KA messages to resynchronize to the network.

4.1.6 TSCH MAC Deficiencies

Although TSCH MAC design goals are technically promising, however, more studies need to be conducted to test the practical performance of the MAC before using it in commercial deployments across the industrial domain. Some recent studies have been conducted in [149, 142] but they only focus on analytical models and simulations. They do not provide realistic performance in experimental set-ups. Only a very few testbed studies have been conducted which can be found in [150, 151]. More experimental studies are required to test the performance of the MAC to be successfully deployed in IWSAN applications.

One important feature which is missing in TSCH is the provision of communication schedule. There is no mechanism that can help to build and maintain communication schedule. Although TSCH defines how to execute centralized, distributed schedule, yet building and maintaining an optimal and reliable communication schedule is still an open research problem [152]. Several studies related to link scheduling have been carried out, which can be found in [153, 154]. Further, TSCH network formation involves transmission of EBs, but the standard does not mention and specify mechanism related to the EB advertisement and configuration [155]. To overcome this issue, a model based optimal beacon scheduling algorithm has been proposed in [156].

Other works in [157, 158] studied performance of TSCH protocol in co-located environments, where multiple instances of the protocol were executed in different neighboring networks taking clock drifts into account (see Chapter 6). Authors revealed that the protocol faces periodic interference that results collision from other nearby networks which deteriorates its performance for reliability. They showed that as the density of the network increases or the number of networks grows the collisions occur more frequently. Further, the recent efforts are to integrate IPv6 with TSCH as explained next.

4.2 6LoWPAN

The underlying motivation to standardize 6LoWPAN [30, 159] was the need to integrate constrained devices to the Internet. IETF created the 6LoWPAN and Routing Over Low-Power and Lossy Networks (ROLL) [21] working groups with the goal toward standardized IP-based protocols for LLN. The ROLL focuses on developing routing solutions for LLNs over IPv6. The fact that the IPv6 protocol imposes high overhead and complexity which makes it difficult to be deployed in constrained environments, such as the IEEE 802.15.4 network. Since the MAC payload of IEEE 802.15.4 cannot be larger than 127 bytes, the 40-byte header of IPv6 does not leave much space for actual payload. This prompted the need to form an adaptation layer between the network and data link layer in order to enable IPv6 packets to fit into the IEEE 802.15.4 specifications as depicted in Figure 4.2. Low-power wireless personal area network impose several constraints, such as small packet sizes, different address lengths, small bandwidth, high density of nodes, battery operated devices, poor link quality, and duty cycling. This makes it challenging to develop an optimized adaptation sublayer to successfully map the service required by the network layer on the services provisioned by the link layer [159].

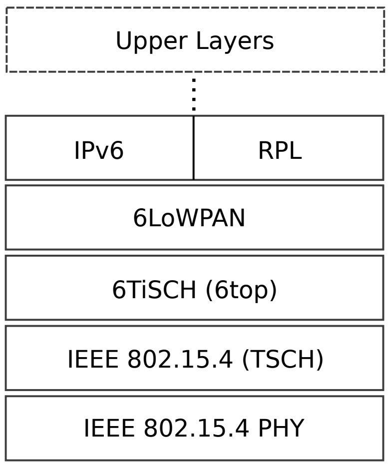


Figure 4.2: The IETF standardized protocol stack for the Industrial Internet of Things.

In essence, 6LoWPAN defines an adaptation layer through *Header Compression* (HC) in order to transmit IPv6 packets over the IEEE 802.15.4 network. It supports packet fragmentation and reassembly in order to meet the *Maximum Transfer Unit* (MTU) requirements of IPv6, and it allows forwarding to the data link layer for multi-hop connections [160]. The 6LoWPAN adaptation layer defines two header compression techniques that compress large IPv6 headers (in the best case) to several bytes.

The compression technique, 6LoWPAN-HC1, compresses IPv6 packets that contain IPv6 link-local addresses. The size of the packet is minimized by eliminating fields such as IP version, traffic class, flow label, and hop limit. The 6LoWPAN-HC2 technique is proposed for the compression of UDP, TCP, and ICMP. The main objective in proposing the HC1 and HC2 techniques was to perform compression in a stateless manner that did not require any previous agreements between the two nodes.

4.3 IPv6 Over TSCH

IETF formed IPv6 Over TSCH (6TiSCH) [161] work group to standardize mechanisms to enable IPv6 over TSCH. 6TiSCH contributes to IoT by bonding the unique features of TSCH and IP networking mechanisms to produce an interoperable IIoT protocol stack [153]. This will support TSCH MAC being placed under an IPv6 enabled protocol stack running 6LoWPAN, IPv6 RPL [162], and Constrained Application Protocol (CoAP) [163]. Figure 4.2 shows the reference protocol stack for 6TiSCH [164]. For successful integration of TSCH with upper layer protocols, 6TiSCH introduces a functional entity that is responsible for scheduling TSCH timeslots to be sent on network. This entity resides at the higher layer and is known as 6TiSCH Operation Sublayer (6top). 6top is a logical link control that resides between the IP layer and the TSCH MAC layer. It controls the TSCH schedule, collects the connectivity graph, and monitors and optimizes the schedule of the cells. It supports both centralized and distributed scheduling approaches. The scheduled cells are labeled as either hard cells or soft cells. Hard cells cannot be dynamically reallocated by 6top. Rather, they are typically scheduled by a scheduling entity such as PCE, that can move or delete cells in the TSCH schedule. In contrast, soft cells can be reallocated by the 6top dynamically. Typically, a distributed scheduling entity schedules these cells. 6top records the performance of the cells to the same neighbor. If a cell performs poorly compared to the other cells with the same neighbor, it moves the cell to a different channelOffset and slotOffset, where channelOffset and slotOffset perform better. In this way, the 6top sublayer can cope with interference reliably.

4.4 IPv6 Routing Protocol for Low-Power and Lossy Networks

IPv6 Routing Protocol for Low-Power and Lossy Networks (RPL) is a a simple interoperable networking protocol standardized by the IETF under the RFC6550. The protocol is specifically designed for resource constrained devices to support multi-hop networks in a wide spectrum of interconnected IoT applications such as industrial, home, and urban applications.

RPL is distance vector routing protocol that constructs a tree like topology called Directed Acyclic Graph (DAG) based on chosen link costs, routing metrics, and constraints. The DAGs are rooted at what is called Destination-Oriented Directed Acyclic Graph (DODAG) which is also known as a DODAG root or a Border Router (BR) in the RPL terminology that connects to the backbone network [165] as depicted in Figure 4.3. For communication among the nodes,

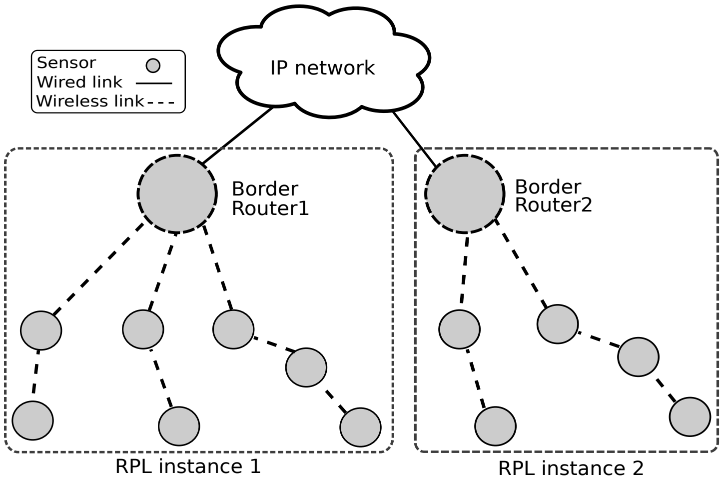


Figure 4.3: A general structure of RPL DAG with two border routers in two RPL instances.

different traffic patterns are supported by RPL such as point-to-point, point-to-multipoint, and multipoint-to-point. Each node transmits DODAG Information Object (DIO) messages to advertise its metrics and constraints. The DIO messages carry information such as rank, DODAG ID, set of candidate parents. A rank determines relative routing distance (for example, hop count) of a node towards BR. A new node that joins the RPL first listens to receive DIO messages which are periodically broadcast by neighbors nodes when their TrickleTimer expires [166]. Once the node receives the DIO message, it selects routing parent as per the requirements of its objective function, routing, and rank information and then forms the routing topology (DODAG) this is how they establish path towards the BR [167].

When a node does not receive any DIO message, it broadcasts DODAG Information Solicitation (DIS) message which forces its neighbor nodes to transmit DIO messages. A notion of RPL instances is used which allows an RPL nodes to participate in multiple DODAGs that share common routing policies. Each RPL instance has its own objectives function for route building. Multiple RPL instances may coexist concurrently in a given topology and a node may participate in more than one instances. These multiple instances help to meet different QoS (e.g., delay, energy) for different routes and traffic flows even for the same destination.

4.5 Conclusions

In this chapter, we exposed the standardization efforts by IETF that contribute to support requirements of LLNs for IIoT. In particular, we elaborated TSCH working details, its scheduling, synchronization, and network formation. We talked about 6TiSCH groups that make efforts to integrate TSCH with IPv6 to foster convergence between low-power networks and the traditional IP networks. We discussed about the routing protocol suitable for resource constrained node. All these efforts help accelerate the efforts towards realizing IIoT.

CHAPTER 5

Evaluation Tools and Metrics for Low-Power Networks

THIS chapter takes you into the domain of performance evaluation which is crucial to understand the key performance indicators of any network, protocol, or algorithm. It provides an overview of the evaluation tools and metrics that have been used in this thesis. We discuss methods and metrics that are used in performance analysis of low-power networks. Our focus is computer simulation, which is a low-cost and less laborious method compared to real-world experimentation. Several simulation tools, that are widely used for protocols analysis, have been presented. We are interested in MAC layer, thus associated with MAC are performance metrics that help determine how a MAC functions as per application requirements. Wireless low-power networks are different from wired computer networks, therefore we define performance metrics that are commonly used in MAC performance analysis.

Section 5.1 gives a general overview of performance evaluation and validation methods, it talks about theoretical, measurements, and simulation methods. Section 5.2 describes performance metrics that are crucial to determine MAC performance. It specifically talks about metrics, that we chose for MAC evaluation in this thesis. Results collection, interpretation, and visualization are part of Section 5.3. Finally, we conclude the chapter in Section 5.4.

5.1 Performance Evaluation Methods

Verification and validation of any proposed protocol or algorithm is necessary so as to examine its performance under certain constraints for which the protocol is developed. This leads to the area of performance evaluation, which is fundamental to developing and analyzing new communication protocols. Performance evaluation has been applied to computer networks and protocols since decades which involves testing them prior to their deployment in real-world applications. Thus, it ensures that the protocol serves at its best through the life-cycle of its operation. It equally applies to the domain of Low-Power and Lossy Networks (LLNs) which involves constrained sensor nodes. Consequently, saving resources and meeting QoS criteria are not only imperative but also challenging aspects of protocol performance.

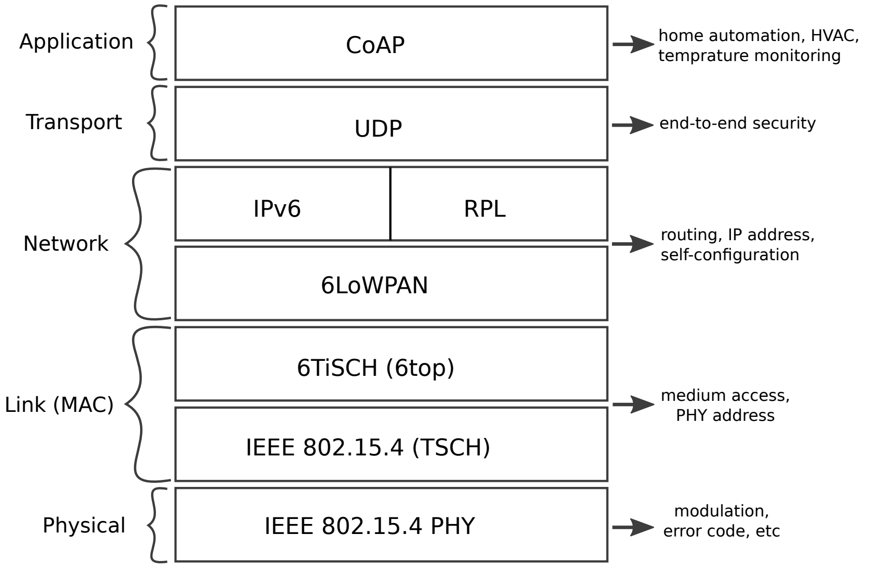


Figure 5.1: A modular protocol stack of IoT defined by IETF [161].

The core foundation of IoT and LLNs depends on software, network, and embedded engineering. Although, these fields are well developed but they need to adapt certain practices and methodologies as per the specifications of wireless LLNs [168]. Over the years, most of the solutions tailoring to the Internet of things are based on the modular protocol stack as depicted in Figure 5.1. Thus, as per the application requirements, appropriate protocols and standards may be selected prior to actual deployment. In this way, deployment cost and efforts can be reduced by allowing several applications to operate on top of the same wireless infrastructure [169]. In particular, agile methodologies are suitable in the development of IoT research solutions as they involve repetitive development life-cycle which has the advantage of quickly rectifying errors during the conception or in the assumptions. Generally, research pertaining to LLNs follows certain repetitive steps similar to one mentioned in [168] as given in Figure 5.2. These steps are needed to conduct performance evaluation of a protocol, an algorithm, or an entire networking stack. Often, neglecting certain steps, for example, making quick transition from protocol idea to hardware experiment evaluation may lead to inappropriate results.

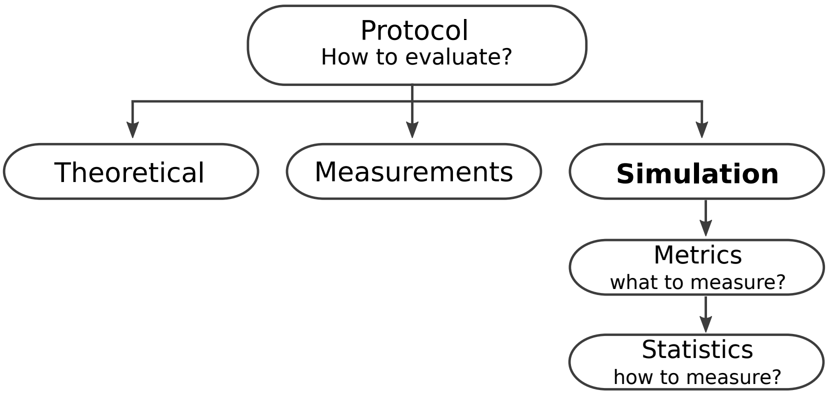


Figure 5.2: Different approaches of protocol performance evaluation.

Generally, there are three common approaches to conduct performance evaluation of a protocol: theoretical analysis, measurements, and simulation. All these techniques come up with their own strengths and limitations, which technique is appropriate, when and how to apply it, is widely discussed in literature [170]. Our work involves theoretical analysis, followed by mathematical analysis to some degree, and then extensive simulations are performed for protocol evaluation.

5.1.1 Theoretical

Often the first step is to evaluate the proposed protocol by examining it theoretically. Although, it is considered preliminary step, yet it helps prove convergence of the protocol or algorithm which ensures that the design is correct. Typically, certain properties are respected such as approximation, lower and upper bounds, complexity, etc. [168]. This approach deals with mathematical abstractions, deriving formulas that best describe performance of a system or protocol. Theoretical analysis is performed when real measurement is not available, but it requires rigorous mathematical background. In terms of efforts and cost, this is the most convenient approach, however it offers limited insights followed by certain assumptions [171]. This is the first step which is later validated by either simulation or measurement/experimental work [170]. Theoretical analysis does not have to be complex, often an available probability distribution function can help do job of model fitting on it. We have seen examples of deriving simple models of traffic generators from the user behavior.

5.1.2 Measurements Analysis

This approach undertakes existing instance of the actual system to conduct performance measurements. This approach produces highly reliable results because the measurements are taken on the system itself, however it is very expensive and takes more time because it requires costs associated with hardware, installation, maintenance, and staff. This method is not always possible, because it may be the case that the system may not yet exist.

5.1.3 Simulation Analysis

Simulation has been widely used for protocol validation over the decades. It involves developing computer programs that are used to implement a system or protocol and perform experiments by running those computer programs [171]. This approach is less expensive and reliable alternative when analytical models or experimental approaches are not directly suitable. It is often the case in protocol development that once it is simulated, it can be later tested through real hardware experiment. However, dealing with hardware experiment is costly and laborious as it requires precise calculation and sometimes controlled environment to accomplish reliable results. The decision to perform simulations only or both the simulation and real-world experiment/measurements largely depends on the nature of the protocol requirements and its underlying complexities. Various simulation platforms have been developed such as OMNeT++, Cooja, OpenWSN, MATLAB, NS-2, NS-3, etc.

There are different types of computer simulations such as discrete-event, Monte Carlo, continuous, trace-driven, and spreadsheets, etc. Discrete event simulation is widely used technique in low-power networks. Discrete-event simulations follows certain sequence of events that take place in a chronological order. It is called discrete event owing to the fact that the occurrence of events or change of states in simulation takes place at distinct points in time. Thus, it offers simplicity and modularity in the evaluation process and protocol can be studied under different conditions. A further benefit of simulation is repeatability, which allows different protocols to be evaluated under precisely the same (random) environment parameters [171].

Particularly, the simulation of LLNs, involves the use of PHY models which includes various radio propagations, however, it is too complex to capture the radio characteristics [172] as it shows dynamic behavior in different environments like indoor, outdoor, urban, and rural. Moreover, most of the simulators do not take into account all the characteristics of specific hardware, and often lack fine grained modeling behavior. For example, clock drift is often not taken into account in simulations which significantly impacts behavior of a protocol, and this is thoroughly discussed in Chapter 6.

Emulation

Compared to simulation, emulation takes into account a fine grained model which is hardware specific. Emulation offers more realism than simulation and provides greater reusability, which means the same implementation can be used not only on emulated nodes but also on real hardware [168]. Thus, it sufficiently reduces the development costs. Most of the development efforts in LLN utilize two frequently used emulators: Cooja and OpenWSN.

Throughout this thesis, we perform extensive simulation-based experiments to test performance of MAC protocols in different scenarios with different parameters. In Chapter 6 and Chapter 7, we use Cooja simulation tool for the performance evaluation of TSCH protocol in different scenarios with different parameters. Likewise, in Chapter 8, we implement and evaluate DMTS-MAC on OMNeT++ together with INETMANET framework. A brief description of OMNeT++ along with its frameworks and Cooja is given below.

OMNeT++

OMNeT++ [173] is not a simulator itself, rather it is an open source discrete event simulation library and framework, which is component-based and extensible. It is widely used for building simulators for modeling and evaluating queuing and distributed wired and wireless communication networks [173]. It is implemented in C++ and has a rich integrated development and graphical interface, which helps design, run, evaluate, and trace simulations. The structure of the OMNeT++ model is based on modules, that can be reused in different ways same as LEGO blocks which makes it more modular. It allows unlimited modules nesting, with which several simple modules can be combined to create compound modules. A simple module is written in C++ together with simulation class library provided by OMNeT++. Communication between the modules takes places via message passing and these messages may contain arbitrary data structures. Depending on the model under consideration, these messages serve as jobs, events, packets, or commands, etc. Modules have input and output interfaces called gates. A link between input and output gates is called connection. In this ways, connections can be assigned different parameters such as propagation delay, bit error rate, data rate, etc. [173]. Similarly, modules can be assigned different parameters that help configure module behavior and customize model topology. An OMNeT++ model is described in NEtwork Description (NED) language, which is a Domain Specific Language (DSL) [171]. It provides extensive random number generating distributions and the ability to perform parallel simulations. OMNeT++ provides support for collecting, analysis, and visualization of simulation results contained in scalar and vector files. Python support is also underway for results processing and analysis, in this way several python-based packages can be used for easy result plotting and visualization.

OMNeT++ supports various ways to run simulations such as graphical and command line interfaces, the former is useful for demonstration and debugging whereas the latter is preferred for batch execution [173]. Based on OMNeT++, several independent simulations models and frameworks have been developed such as INET, INETMANET, Castalia, OverSim, and MiXiM as discussed below. These frameworks and models are now commonly used to test different types of protocols and networks.

INET

INET [173] is a widely used simulation package as it contains several Internet protocols and other models to perform simulation particularly in communication and networking. In this way, it helps evaluate and validate new protocols in different scenarios [174]. Often the latest frameworks and models take INET as a base and build on it to simulate more complex networks and protocols.

MiXiM

MiXiM [175] is a simulation package based on OMNeT++, which was primarily used for simulation of wireless and mobile networks. It is a merger of several frameworks such as ChSim, MAC simulator, Mobility framework, Positif framework. Several other projects have been integrated into MiXiM such as EnergyFramework, CSMA module, IEEE 802.15.4 and IEEE 802.15.4 modules, BaseMacLayer, L-MAC, MoBAN (Mobility Model for Body Area Networks), Flooding network layer, WiseRoute network layer, ProbabilityBroadcast network layer modules, and Analogue Models: BreakpointPathlossModel and PERModel. Therefore, it features detailed wireless channel models, mobility models, obstacles models, and numerous protocols, particularly, it has a great support for MAC layer. MiXiM is now deprecated and all its contents have now been merged with INET since INET-3.x version [176].

INETMANET

INETMANET [177] framework offers similar features as the INET framework but extends INET by providing increased support for simulating Mobile Ad Hoc NETworks (MANETs). It was initially a fork of the INET. It supports several protocols such as AODV, OSLR, DSR, and others. INET's first version had limitations for link layer and routing protocols for simulation of MANETs. INET-MANET overcame those limitations by including support of IEEE 802.11a/g/e and 802.15.4 (now they are also part of INET) [174]. In this way, it supports low-power IoT networks in more realistic scenarios. As MiXiM is no longer maintained, so several propagation models developed for MiXiM are now part of INETMANET. The initial version of INET did not have energy producer and consumer model. INETMANET uses MiXiM models and adapted them to facilitate energy consumption simulation of wireless networks. Several link layer models have been included in INETMANET which cannot be found in INET. Certain simulation models and implementation codes which were originally written for INETMANET, they have been included in INET as well. INETMANET is being actively maintained and developed with major difference to INET with respect to routing protocols, mobility models, application models, interference models, etc. [174].

Cooja and Contiki

Contiki-OS

Contiki is an operating system [178] that provides hardware and software support for LLNs platforms. It is open source that enables low-power IoT devices to connect to the Internet. Contiki offers fully standard network stacks such as uIP with the support of standard protocols such as IEEE 802.15.4, 6LoWPAN, TSCH, 6TiSCH, RPL and CoAP. Conitki provides easy and fast development of applications which are written in C. After Contiki version 3.0, it is no longer maintained, rather a new Contiki-ng [179] called next generation OS for IoT, has been developed which is a fork of Contiki-OS.

Cooja

Cooja is a network simulator within Contiki-ng, that has capability to emulate real hardware platforms. It is extensively used to simulate small and relatively large wireless networks of low-power and low-cost embedded sensors and actuators called motes. It helps develop, validate, run, and debug protocols and applications. Researchers and developers can build and test networks and protocols with Cooja emulated motes before actually running them on real hardware. The code which is executed by the motes is exactly the same firmware that you may upload on the physical devices. Cooja is based on Java and has a graphical interface. It is extensible and supports various widely used hardware platforms such as CC2420, CC2650, Zolertia Zoul, openmote, native Cooja motes, nrf52dk, NXP jn516x, Tmote Sky/TelosB, and several others. It includes various propagation models such as Unit Disk Graph Medium (UDGM), distance loss UDGM, Directed Graph Radio Medium (DGRM), Multipath Ray-tracer Medium (MRM). It also has support for the integration of external tools and plug-ins to provide additional features for networks, protocols, and applications. Two such plug-ins are mobility plug-in and interference plug-in, which help emulate behavior close to reality.

Cooja is currently the most dominant tool used by researchers and developers for simulation and emulation of LLN networks as can be seen in Figure 5.3 which is adopted from [165]. It depicts that 62.9% simulation studies related to Contiki-rpl were conducted using Cooja [165]. This is based on results of 97 research publications between 2010 to 2016 found in IEEE Xplorer, Google Scholar, ACM Digital Library, and IETF RFCs. Cooja/Contiki is actively maintained and supported by the community, this is the reason that most of the latest IETF drafts are often available for them.

Cooja Mobility Plug-in

This plug-in was developed by Fredrik Osterlind which allows nodes to move in different directions within a network. The positions of nodes are stored in a file called position.dat. The file is first loaded in the simulation before the simulation starts. A typical example of node position formate inside the file is given as follows.

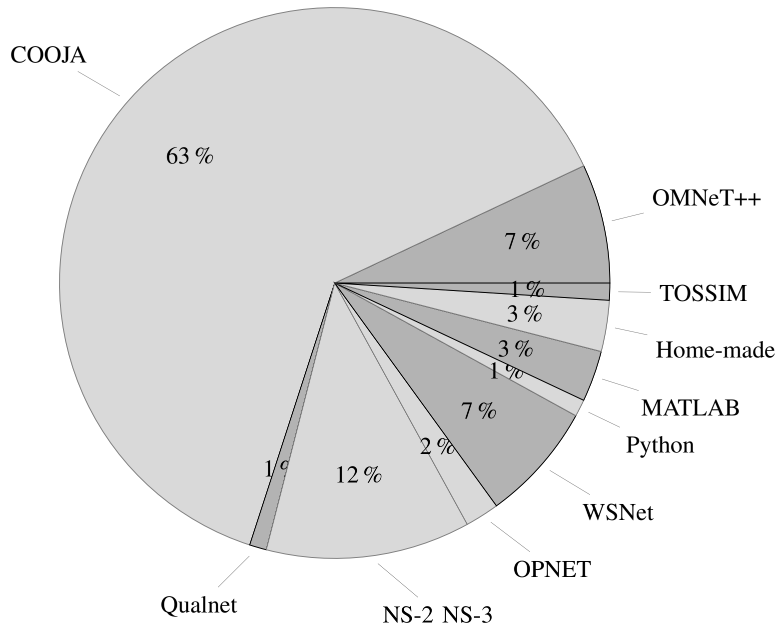


Figure 5.3: Usage of different simulators in RPL-based low-power and lossy network implementations.

Node#	**Time(s)**	**x**	**y**
0	0.000	1	0
1	0.000	2	0
0	0.250	1.50	0
1	0.250	2.50	0
0	0.500	2	0
1	0.500	3	0

The first line means that the node 0 at 0.0 second will be located at the position coordinates (1, 0) and node 1 at 0.0 will be positioned at coordinates (2, 0) and so on.

We use mobility plug-in for Cooja for the evaluation of TSCH protocol under node mobility as detailed in Chapter 7. The mobility plug-in enables nodes to move in the network with the option to support different speeds of movement.

Comparison of Simulation Tools

Table 5.1 depicts comparison among aforementioned simulation tools based on different features.

Table 5.1: Comparison of different simulation tools based on different features.

Simulator	Simulation type	Language	License	GUI
Cooja	Discrete event	C	Open Source	Yes
OMNeT++	Discrete event	C++	Open/Commercial	Yes
TOSSIM	Discrete event	nesC	Open source	No
NS-2	Discrete event	C++/OTcl	Open source	Limited
NS-3	Discrete event	C++	Open source	Yes
MATLAB	Event driven	C/Java	Commercial	Yes
Qualnet	Discrete event	C++/Parsec	Commercial	Yes
WSNet	Event driven	C++	Open source	Yes
OPNET	Discrete event	C/C++	Commercial	Yes

5.2 Metrics

The performance evaluation of MAC protocols undertakes certain performance metrics or factors, which define a criteria that should be measured to analyze their performance. Thus, determining performance metrics is inherent and imperative part of MAC protocol development, however, the choice of metrics depends on the application. Below we detail, commonly used metrics that have been part of our research for performance analysis of TSCH and DMTS protocols. It should be noted that these metrics have been commonly used in link layer studies for LLNs.

5.2.1 Packet Delivery Ratio

In various communication networks and protocols, reliability is mostly tied with Packet Delivery Ratio (PDR). As link unreliability, packet collision, or packet loss due to interference is common in low-power networks, thus accurate measure of packet delivery is mandatory. PDR is the ratio of total number of packets received by a destination node to the total number of packets generated by a source node during a given simulation time. Reliability can be as overall or end-to-end, end-to-end PDR undertakes the calculation of PDR at every receiver and transmitted by every source.

In this thesis, we use PDR as a measure to determine reliability of our proposed Dual-Mode Time-Slotted (DMTS)-MAC protocol. We set upper and lower threshold values of PDR that serve as boundary values between reliability and unreliability as detailed in Chapter 8. Due to channel hopping, DMTS-MAC improves end-to-end reliability by using different channels at each timeslot. A node, using DMTS-MAC, generates and transmits its packet to its immediate parent in its dedicated timeslot which is forwarded by next parent in a multi-hop fashion which is finally received by the sink. We calculate PDR by counting total number of packets received at the sink to the total number of packets generated by each node in the network. We undertake overall reliability which seems straightforward without the burden of counting packets at each sender and receiver. We measure PDR in the presence of interference to see how DMTS-MAC performs in a scenario which is close to reality.

In Chapter 7, we analyze reliability of TSCH protocol under node mobility so as to determine how the protocol performs when nodes are mobile. We calculate how many Keep-Alive (KA) messages are transmitted and lost due to mobility. KA messages are control messages transmitted by a nodes to resynchronize to the network. Chapter 6 evaluates reliability TSCH protocol in co-located scenarios by introducing clock drift. The reliability is determined by calculating the number of transmitted packets and lost packets due to interference.

5.2.2 Delay

Often an end-to-end delay or node-to-node delay is measured. For the successful implementation of a control loop, it is imperative to guarantee an upper bound for the data transfer between sensors and actuators.

One of the core objectives of DMTS-MAC was to reduce delay by not using retransmission opportunity so that fresh data is transmitted with low delay. We measure end-to-end delay which is the total time required for data transmission from sensors to actuators. This delay is deterministic due to pre-allocation of timeslots and frequency channels inside the a superframe. The delay is measured by the duration of timeslot and total number of timeslots inside the DMTS-MAC superframe.

5.2.3 Energy Consumption

Energy consumption is undoubtedly one of the main issues for resource constrained sensor nodes as they are mostly battery powered and battery replacement is often infeasible. Thus, the radio transceiver should be turned-on precisely when a node transmits and receives a packet else it should be tuned-off, however, it is non-trivial to achieve this in practical scenarios. In reality, different states of the radio transceiver consume different amount of energy as discussed in Section 3.4. To overcome unnecessary radio wake-up, duty cycling (DC) is widely used to save energy in which nodes sleep by turning-off their radio related circuity if they do not have packets to transmit or receive. In this way, duty cycling serves an important metric that helps to extend lifetime of nodes. Energy consumption and network life time are closely related and are often interchangeable. Duty cycling is defined as the ratio of total listen interval to total sleep and listen interval as given in equation 5.1.

$$DC = \frac{T_{listen}}{T_{listen} + T_{sleep}} \tag{5.1}$$

Our proposed DMTS-MAC introduces duty cycling by allocating sleep slots in the superframe so that nodes can save energy. A node, using DMTS-MAC superframe, either transmits, receives, or sleeps in its dedicated timeslot. We analyze the energy consumption of the nodes based the number of slots a node is allocated in given superframe cycles. Sleep slots are just the representation of the duty cycling, while we actually calculate the energy of the nodes during transmit and receive slots. Once this energy consumption is known and the initial energy of the nodes, the overall energy consumption can be easily calculated. We use overall energy consumption of nodes as a metric to depict the comparison between available energy and consumed energy.

5.2.4 Scalability

In this thesis, we evaluate scalability of TSCH protocol from two perspectives, one is related to scaling up network by adding more number of nodes, second by increasing number of networks. The evaluations in Chapter 6 increases the number of networks and as well as number nodes to analyze how it affects interference. In Chapter 8, our proposed DMTS-MAC protocol adapts the superframe structure of DMA-MAC to enhance scalability by accommodating more number of nodes while respecting same delay and energy constraints. Scalability is often a challenge for supeframe-based protocols as they are less scalable, for example adding new nodes in network requires the entire schedule of nodes to be updated which incurs additional overhead of energy and delay.

5.3 Result Visualization and Interpretation

Once the performance metrics are selected, the next step to decide on how they should be measured in order to infer certain tendency or make decision on protocol performance from a collected data set of that metric. We use various statistical methods to analyze data gathered from simulations. These include average values, minimum, maximum, variance, interquartile ranges, confidence intervals etc. The data is then visualized graphically to understand tendencies in a concise form to be able to make conclusions. There are numerous ways to plot the data graphically as shown in Figure 5.4 which is adopted from [180]. These graphs help visualize data in a more precise and clear form.

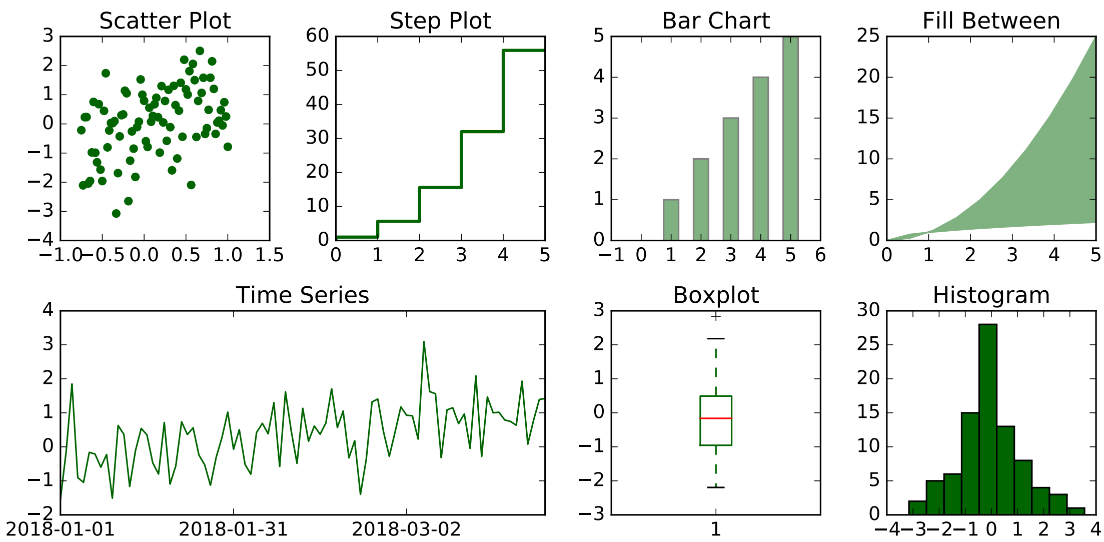


Figure 5.4: Different ways that can help visualize data graphically.

Throughout the thesis, results have been shown with *box-and-whisker* plots, also known as boxplots. Boxplots conveniently depict distribution of data such as minimum and maximum values, interquartile ranges, mean, and as well as the spread or dispersion of the box which can clearly help estimate a tendency more precisely and identify outliers as compared to other form of graphical representations. An outlier is an observation which appears to be far distant from the rest of the data as denoted by small letter x in Figure 5.5. Outliers appear to be outside whiskers in boxplots. A simple boxplot and its associated terminology is explained in Figure 5.5.

The rectangle is called the *box* and the two right and left extremes which show

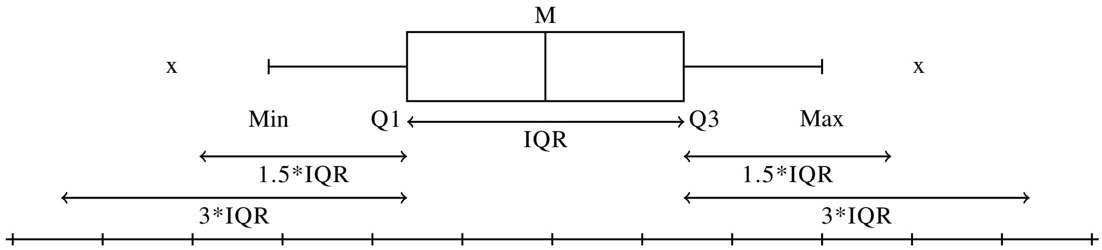


Figure 5.5: Graphical representation through Box and Whisker plot.

smallest and largest observations of data are known as *whiskers*. The *Median* (M) shows mid point of data. The letter Q suffixed with a number represents *Quartiles* (percentiles). Each quartile represents one-fourth of the data. The Q1 is called lower quartile and show 25% of the data set while Q2 is called upper quartile and represents 75% of the data set. The difference between Q1 and Q2 is called Inter Quartile Range (IOR). Boxplots can be drawn vertically or horizontally, and based on convenience they can be scaled differently.

5.4 Summary

This chapter discussed about performance evaluation and how it should be conducted. Various methodologies used in performance evaluation have been thoroughly discussed. In particular, we focused on simulation approach to analyze MAC protocol performance. Several simulation platforms along with their working mechanism were explained with reference to low-power networks. MAC performance metrics that have used in thesis were described, which include, PDR, delay, scalability, and energy consumption. In the end, we illustrated different statistical methods and explained tools that can help visualize data graphically.

CHAPTER 6

Co-located TSCH Networks: An Inter-network Interference Perspective

THIS chapter studies closely co-located TSCH networks from interference perspective and shows how interference impacts TSCH network performance in terms of successful communication and periodic communication blockage. Our results demonstrate that co-located TSCH networks periodically interfere with one another if they do not cooperate.

Section 6.1 gives the introductory perspective on coexistence among low-power wireless networks in a co-located environment and gives a brief discussion on TSCH protocol. Related studies are discussed in Section 6.2. The approach and experiment setup are demonstrated in Section 6.3. The evaluation results are detailed in Section 6.4 and conclusions are drawn in Section 6.5.

6.1 Overview

Recent advances in the IIoT push the need to define new protocols to meet the requirements of its dense deployments. Real-world deployments of industrial low-power networks are expected to integrate multi-vendor solutions. Most of these solutions prefer wireless communication based on different standards such as IEEE 802.15.4, WLAN, WirelessHART, and ISA100.11a and they make use of unlicensed bands and several networks may coexist in close locations. This coexistence of network protocols is prone to creating interference, particularly in urban residential, smart city, and industrial scenarios. Due to high heterogeneity of devices and their ownership, interference across co-located networks emerges as a barrier to guarantee reliability and low energy consumption. Interference indeed causes packet loss which increases the energy for retransmission, hence affects the communication reliability.

Nowadays, most of the evaluation of communication protocols is done in standalone networks. Very little attention is devoted to evaluating their behavior in co-located networks. Though, their performance may be good in an isolated network, yet they may present performance issues when different instances of these protocols are operating in co-located networks in the same physical space. In this chapter, we study performance of TSCH protocol in co-located networks when introducing a clock drift among the networks. As discussed earlier, in practical network deployments nodes encounter clock drifts with respect to one another due to clock imperfections which may cause synchronization problems. Thus, it is one of the important factors to consider in network performance when multiple networks are operating in close proximities. In this way, it enables us to determine a more realistic impact of clock drift on network performance in coexisting environment.

As mentioned before, TSCH MAC mode has received increased attention for IoT, especially in industrial deployments, due to its *time-slotted* structure and *channel hopping* which offer enhanced communication reliability and very low-power consumption [111, 181]. Operating with other constrained protocols such as 6LoWPAN [145] or RPL [21], the full network stack can easily be embedded in any constrained device. Therefore, it satisfies the IoT requirements where nodes are meant to be reliable, mostly battery-operated, and have constrained processing power. Please refer to Section 3.4.5 for a detailed working of TSCH protocol, its slotframe structure, synchronization mechanism, and network formation.

6.2 Related Studies

In this section, we give a brief discussion of the related work regarding interference in coexisting networks. There are several research studies that presented the problem of inter-network interference and coexistence especially between the IEEE 802.15.4 and the IEEE 802.11 networks [182]. Only a couple of works focused on the interaction between co-located IEEE 802.15.4 networks that overlap in communication and interference ranges [183] [184] [158].

Nordin *et al.* [184] studied multiple co-located IEEE 802.15.4 wireless PANs and tried to quantify the impact on network performance. The authors showed that when multiple PANs coexist independently and unsynchronized, they resulted in beacon collisions. They demonstrated that network experienced considerable beacon loss and emphasize on the need to coordinate beacon scheduling through adaptive schemes in inter-network operations.

Feeney *et al.* [183] performed a comprehensive simulation study on the inter-network interactions between two co-located IEEE 802.15.4 beacon-enabled PANs. The authors revealed complex behaviors that showed large and slow oscillations in throughput: slow deterioration and recovery. Authors pointed out that the networks experienced slow oscillations in packet reception rate in different periods and sometime complete packet loss.

Another work that studied the inter-network interference between TSCH networks is given in [158]. In this work, a variable number of synchronized and unsynchronized instances of the TSCH networks were investigated experimentally. The results indicated that when there were multiple TSCH networks with high traffic load, they faced collisions due to inter-network interference causing network performance to decrease. While this study tried to show the traditional metrics such as packet delivery ratio, we take a different approach and take into account successful communication ratio as the desired metric.

6.3 Approach and Experiment Set-up

The evaluations are performed through simulations for which we use the Cooja network simulator which is part of the Contiki-OS [179]. We use the RPL-specific [21] approach, which is commonly preferred for IoT networks.

In RPL, the network nodes associate with a coordinator called the border router. In a typical scalable sensor network deployment, all nodes are not directly interacting with the application. Instead, traffic is directed toward a sink node, acting as a gateway to the outside world. To emulate upward traffic configuration appearing in sensor network deployments, packets are generated mostly periodically from all nodes toward the border router. For our experiments, the traffic generation period is set to 1 second. To analyze the effect of intra- and inter-network interference, the simulated transmission success ratio is set to 100%, meaning that the outside environment has no impact on the transmission. In this configuration, a connection is treated as **unsuccessful** only when there is interference created by the nodes and which is blocking the communication process. To evaluate the impact of intra-network interference which is the interference within a network and inter-network interference which is the interference between the networks due to their co-location, we analyze all packets exchanged between the nodes including acknowledgments and EBs. The IEEE 802.15.4-TSCH protocol schedules the slotframe in order to achieve reliable communication. Active research is ongoing to find the best scheduling algorithm but no specific scheduling algorithm is defined by the standard. However, a default slotframe schedule namely minimal TSCH (*TSCH_min*) is available (see Section 4.1.3).

For our experiments, we use TSCH_min as configured in [145], thus with 11 timeslots. With only one shared slot available to transmit data and EBs, TSCH_min is prone to creating interference. In this study, we analyze interference resulting from the network, and interference created by the co-location of other networks. For a network n of a set of networks N at time x, non-interfering connections (or *Successful Connections* (SC)) can be seen as a time-dependent process $SC_n(t)$. The average number of non-interfering connections is given by

$$SC'(x) = \frac{dSC_n(x)}{dt}$$

A connection is successful when the communication between two nodes of the same network is not impacted by any other transmission occurring at the same time. To estimate the amount of non-successful connections in a network, we compare the previous defined value to the total number of connections given by

$$TC(t) = \sum_{n \in N} SC_n(x)$$

The average number of total interfering connections is given by

$$TC'(x) = \frac{dTC(x)}{dt}$$

We define the **Connection Success Ratio (CSR)** in total at time t, given by

$$CSR(x) = \frac{dSC(x)}{dTC(x)}$$

A connection success ratio equals to 1 means, for the time interval dt considered, all connections are successful. Similarly, a connection success ratio equals to 0 means, for the time interval dt considered, all connections interfere. This ratio, representing the ratio of successful connections will be our metric to compare the amount of interference occurring in a network.

6.4 Results and Discussions

The result section is divided into three sub-sections. In the subsection 6.4.1, we use the CSR metric to analyze interference occurring in two simple co-located networks composed of two nodes each. In the subsection 6.4.2, we increase the number of channels used to measure its impact in terms of interference mitigated. In the subsection 6.4.3, we analyze the behavior of networks coexisting when the size of the network increases, and when the number of networks grows.

6.4.1 Two PANs Topology

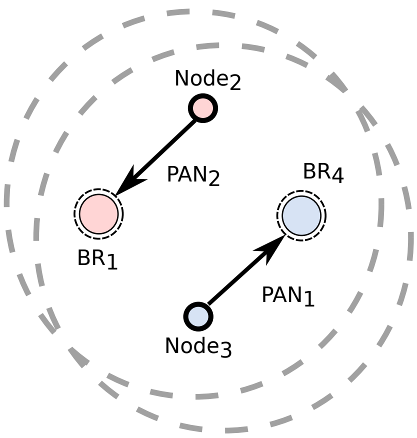
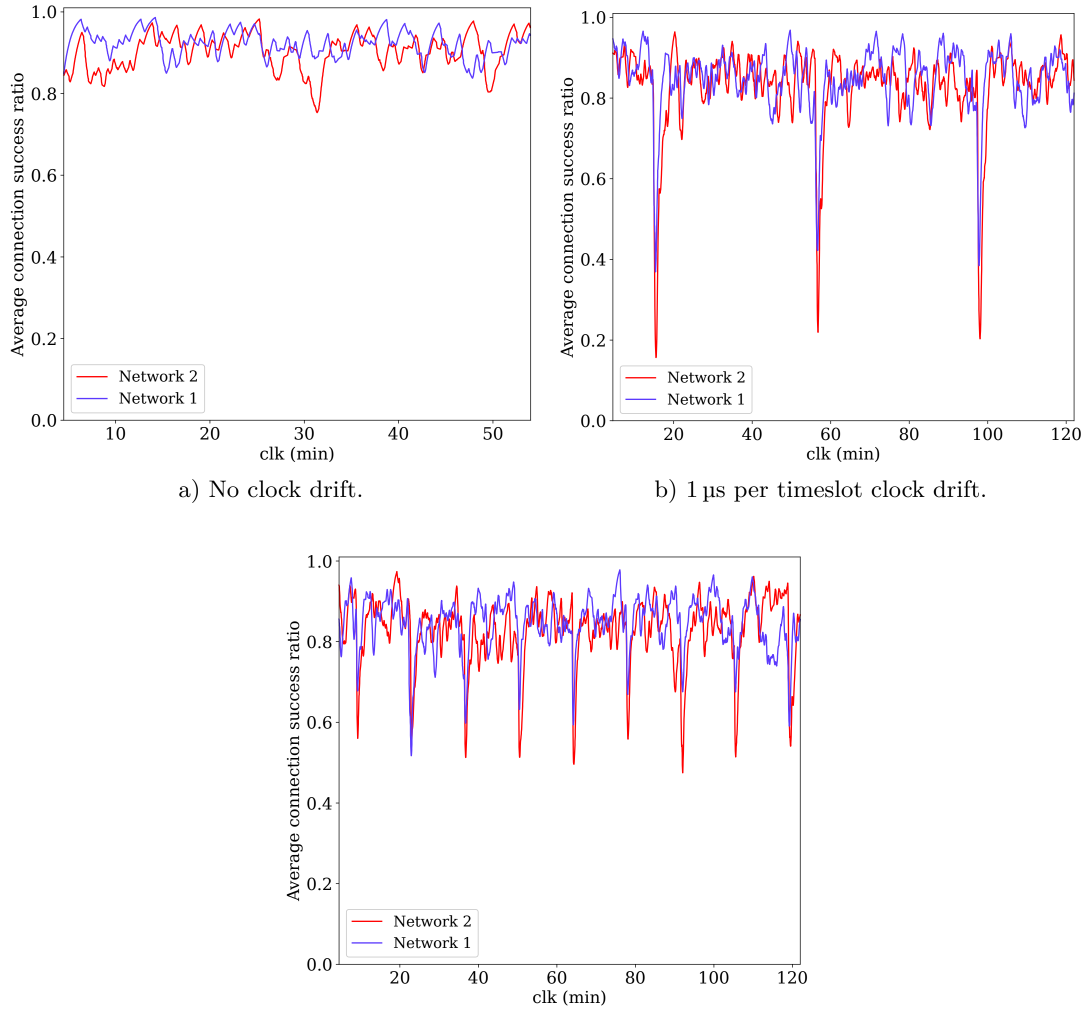


Figure 6.1: Two PANs topology, the dotted circles show the interference range and the communication range overlapping for both networks.

Our first experimental scenario undertakes the impact of interference when two personal area networks are closely co-located as depicted in Figure 6.1. The reason to use this stylized simple networks is to have minimal impact on link quality variations, the effects of varying interference, in-network contention, and unfairness for shared slots and demonstrate interference in different modes of interactions. We set both networks to be in each others' transmission range as well as interference range to see interesting behaviors. In the first part, only one channel is used in order to emphasize the interference situations. Both networks are synchronized based on the border router's clock. Depending on the hardware used, these clocks can drift with time. Typical IEEE 802.15.4 devices having 32 MHz clock with 30 ppm (parts-per-million) may drift up to 60 µs per second [185]. In Figure 6.2, three different situations are considered.

In Figure 6.2a, there is no drift between clocks. In this scenario, there is a high probability of having no inter-network interference due to the random start-up offset of both border routers. Therefore, connection success ratio of both networks



a) No clock drift.

b) 1 µs per timeslot clock drift.

c) 3 µs per timeslot clock drift.

Figure 6.2: Moving average of the connection success ratio of both TSCH networks with a random clock offset, and different clock drift situations.

seems to oscillate around 0.93 meaning that in average, 93% of all connections are successful. Whereas the loss of remaining 7% CSR is due to intra-network interference.

In Figure 6.2b, there is 1 µs per timeslots drift between clocks. In this situation, we observe periodic interference every ≃ 40 min represented by a drop of connection success ratio. This is because when the clock drifts, the timeslots align themselves automatically every now and then, thus creating interference.

In Figure 6.2c, there is 3 µs per timeslots drift between clocks and interference seems to occur more frequently.

When there is clock drift between the networks, interference seems to occur periodically. The interference observed is due to the co-location of both networks. When the clock drifts, both networks are artificially synchronized each periodic amount of time. Since TSCH_min provides only one opportunity to transmit per slotframe, this period can easily be calculated. It corresponds to the moment when the clocks are aligned on the first cell of the slotframe. With each timeslot measuring $T_{ts} = 15\,000\,\mu s$ and the slotframe being $T_{sf} = N_{ts} \times T_{ts}$ long, with N_{ts} the number of timeslots in the slotframe, the slotframes are synchronized every time period P in seconds (sec) or minutes (min). Thus

$$P = \frac{T_{ts}}{d} \times T_{sf}$$

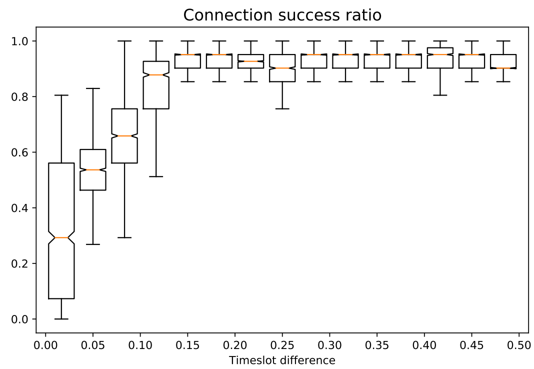
with d the drift per timeslot. With $d = 1$ and $N_{ts} = 11$ for minimal TSCH, we obtain $P = 41.25$ min and with $d = 3$, $P = 13.75$ min. These time periods of P correspond to the observations of Figure 6.2b and Figure 6.2c.

Observations of Figure 6.2 show that inter-network interference is responsible for much more failed connections than intra-network interference. While intra-network interference seems to generate an average CSR of 0.93 in all experiments, inter-network interference generates a significant drop of average CSR. This drop is more significant when the clock drift is lower, because the connections are interfering during a longer time. However, when the clock drift is higher, the drops are occurring more often.

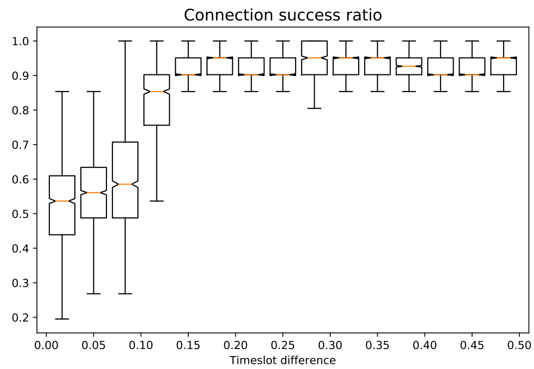
6.4.2 Impact of Channel Hopping

In this experiment, the same two PANs are used but the number of channels differs. Since inter-network interference occurs periodically, we analyze the CSR as a function of the timeslot difference between both networks. This timeslot difference is comprised between 0 (both networks clocks modulo T_{ts} are equal) and 0.5 (both networks clocks modulo T_{ts} differ by half a timeslot). The results are depicted in Figure 6.3. We repeated this experiment thirty times and modified the number of channels used. The channel hopping pattern is random among the available channels.

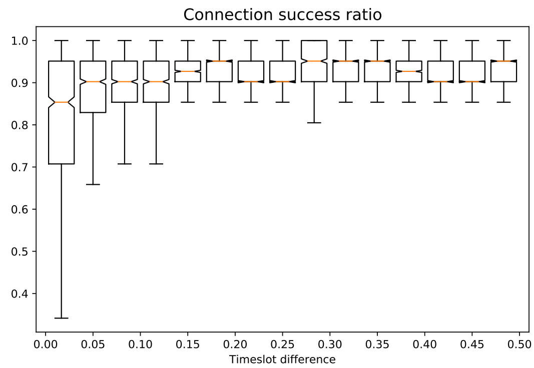
With only 1 channel used, we observe that inter-network interference is occurring only when the timeslot difference is lower than $\simeq 0.12$ timeslot. We observe 0.3 to



a) 1 channel used.



b) 4 channels used.



c) 16 channels used.

Figure 6.3: Boxplots of the connection success ratio as a function of the timeslot difference between both networks.

0.7 CSR. After 0.15 timeslot difference, the CSR reaches its same amount of 0.93 for this topology and schedule. This is due to the fact that the transmission time is approximatively 0.12 timeslot long. After this period, even if the timeslots are overlapping, the transmissions are not interfering. When increasing the number of channels used, the proportion of successful connections also increases. In the worst possible situation, that is when the timeslot difference is 0 with 4 channels, the average CSR raises to 0.55. With 16 channels, the average CSR reaches 0.86 at 0 timeslot difference, which is close to the intra-network CSR measured of 0.93. This means that almost all the inter-network interference is avoided.

Increasing the number of channels allows to make full use of the channel hopping mechanism of TSCH. With channel hopping, intra-network interference still occurs at the same rate because of the structure of the minimal TSCH schedule. However, inter-network interference is avoided since two different networks may not be communicating on the same channel. In our case, the channel hopping pattern is random.

Therefore, there is a theoretical probability of interference event A such that $P(A) = \frac{1}{n_{ch}}$ that two transmissions occur on the same physical channel, n_{ch} being the number of channels used. With more than 2 networks, the probability to have N networks interfering is given by

$$P\left(\bigcup_{i=1}^{N-1} A_i\right) = \sum_{k=1}^{N-1} P(A_i) - \sum_{i<j} P(A_i \cap A_j) + \sum_{i<j<k} P(A_i \cap A_j \cap A_k) - \cdots + (-1)^{(N-1)-1} \sum_{i<\cdots<N-1} P\left(\bigcap_{i=1}^{N-1} A_i\right),$$

which, in a closed form, becomes [1]

$$P\left(\bigcup_{i=1}^{N-1} A_i\right) = \sum_{k=1}^{N-1}\left((-1)^{k-1} \sum_{\substack{I \subseteq \{1,\ldots,N-1\} \\ |I|=k}} P(A_I)\right) \qquad \forall I A_i = \frac{1}{n_{ch}}$$

Then,

$$P(A_I) = \frac{1}{(n_{ch})^{|I|}}$$

Here, $P(A_I)$ is the set of neighboring networks. Therefore, having more available physical channels than co-located networks is crucial.

6.4.3 Scalability

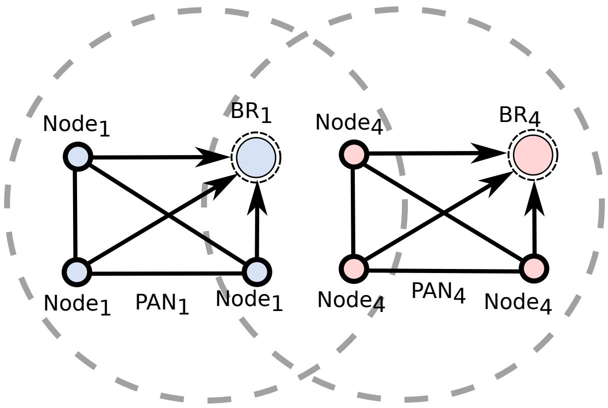
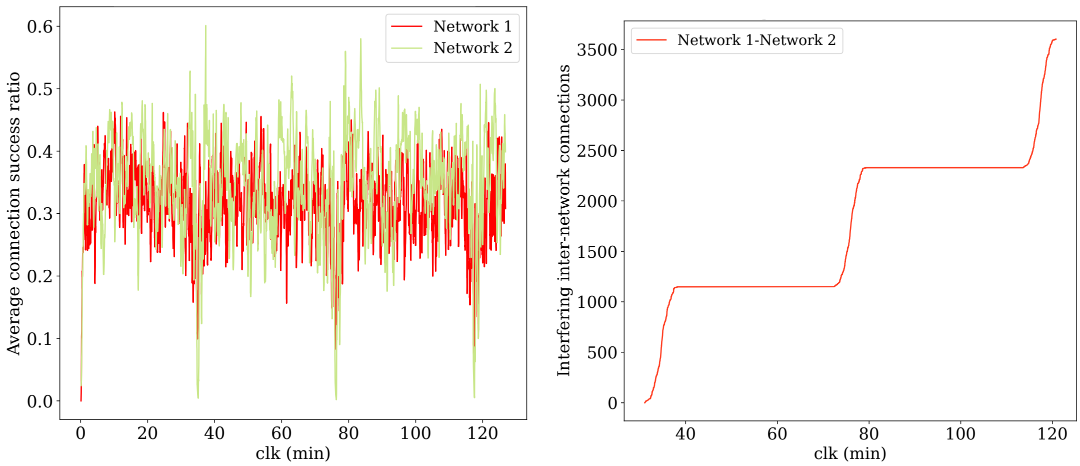


Figure 6.4: Two PANs topology, each with four nodes, the dotted circles show the interference range and the communication range overlapping for both networks.

[1] https://www.wikiwand.com/en/Inclusion%E2%80%93exclusion_principle#/In_probability

In order to study the impact of scalability on inter-network interference, two different topologies, as shown in Figure 6.4, are tested with only one channel in use. In this case, scalability refers to scaling up the networks in terms of adding more number of nodes. We first increase the number of nodes in each network. The drift is 1 µs per timeslot. The results are presented in Figure 6.5. With minimal TSCH schedule, increasing the number of nodes drastically increases the amount of interference within the network.



a) Connection success ratio. b) Amount of interfering connections.

Figure 6.5: Experimental results of 2 networks of 4 nodes each.

Presented in Figure 6.5a, the average CSR oscillates around 32%, meaning that only one packet out of 3 is successfully transmitted due to intra-network interference. We also observe a periodic drop of CSR due to inter-network interference. Similarly as with two nodes, both networks are artificially synchronized every 41 min, creating this periodic pattern. This pattern is confirmed when observing the amount of interfering inter-network connections in Figure 6.5b.

While the pattern is similar to the first experiment, the amount of interfering connections is much more significant when the number of nodes increases. In this topology, when the networks are artificially synchronized, approximately 1000 connections interfere, while approximately 300 connections with only two nodes. In bigger networks, more messages are generated to successfully transmit data packets due to the design of the minimal TSCH slotframe. Coupled with routing messages generated by RPL, the amount of transmissions is more important in this topology.

We also analyzed four networks composed of two nodes in each network as depicted in Figure 6.6. In this case, scalability refers to scaling up the number of networks in order to see how increasing the number of networks impacts interference. In this configuration, every network is generated with a different drift, from 0 to 3 µs per timeslot for the Networks 1 to 4 respectively. This allows

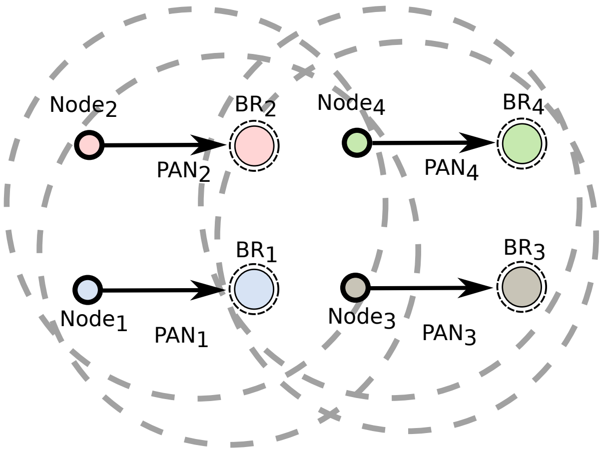
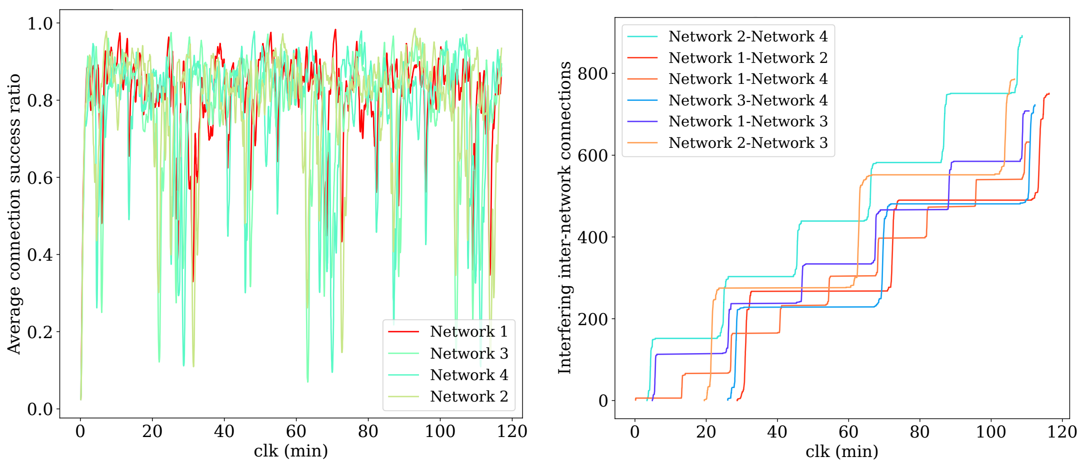


Figure 6.6: Four PANs topology each with two nodes, the dotted circles show the interference range and the communication range overlapping for all networks.



a) Connection success ratio. b) Amount of interfering connections.

Figure 6.7: Experimental results of 4 networks of 2 nodes each.

to emulate a real co-located TSCH deployment where different border routers have different clocks. The amount of inter-network connections and CSR are presented in Figure 6.7. Due to the different drifts, each network interferes periodically with every other network. This behavior is represented in Figure 6.7a with periodic drop of CSR. However, since these networks are smaller, less packets are generated and interfering connections have less impact on the CSR metric. As depicted in Figure 6.7b, Network 1 and Network 2, which have a 1 µs clock drift between them, generate only 300 interfering connections, 3 times less than the previous experiment. We also notice that, the more frequent the inter-network interference occurs, the more interfering connections it creates.

From the two experiments with 4 nodes, it appears that increasing the number of networks generates much more inter-network interfering connections than only with two networks. After 2 hours of experiment with two networks, the total of inter-network interfering connection is $\simeq 3500$, while with 4 networks we reach 4400.

6.5 Conclusions

In this chapter, inter-network interference among several co-located TSCH networks was studied. With the CSR metric, we analyzed the proportion of successful connections at each time. This metric showed that TSCH networks, scheduled with the minimal TSCH, experienced significant interference. Although, other scheduling algorithms might present better performance in terms of intra-network interference, yet the inter-network interference would still occur because both networks schedule communications on a slotframe which repeats over time. Co-located networks with the exact same clock will not interfere among each other if their timeslots are not aligned. However, in a real deployments, hardware clocks drift by a small amount and this creates periodic inter-network interference. When increasing the number of nodes, more interference appears periodically. Depending on the clock drift between both networks' coordinators, this may create significant down-time in the network. Increasing the number of networks causes inter-network interference to occur more frequently.

Co-locating TSCH networks becomes a more challenging problem especially in industrial networks because different hardware vendors are unlikely to share their network stacks. To cope with this problem, our results showed that all 16 channels must be used when configuring TSCH because this contributes greatly to reducing inter-network interference. Furthermore, the number of TSCH networks must be kept as small as possible. Ideally, all devices should be part of the same network and be synchronized on the same clock to avoid clock drift, however, this requirement is hard to fulfill in large scale deployments due to tight synchronization requirements of TSCH.

CHAPTER 7

Reliability Analysis of TSCH Protocol in a Mobile Scenario

IN this chapter, we analyze the reliability of TSCH protocol under node mobility. As mobility is indispensable for future industrial low-power wireless networks to support diverse applications so as to increase operational efficiency and ensure autonomy. Therefore, it is important to present important insights into the TSCH with respect to synchronization loss, message overhead, and delay problems, which are induced by mobility in the context of industrial applications.

We emphasize on the need of mobility for emerging industrial applications in Section 7.1. We provide node mobility related studies in Section 7.2. The description of evaluation through simulation and experiment set-up are given in Section 7.3. We discuss the results in Section 7.4 and conclude the chapter in Section 7.5.

7.1 The Need for Mobility

The growing adoption of industrial low-power wireless networks serves as the backbone for the low-power Cyber-Physical Systems (CPSs). These low-power CPSs are expected to encompass mobile nodes in near future. In this way, they promise to play a remarkable role for the automotive industry where mobile robots embedded with sensors and actuators can collaboratively exchange information to perform operations autonomously. Mobility induces several challenges for low-power lossy networks due to dynamic topology, RF link instability, synchronization loss, signaling overhead, which lead to significant packet loss, more energy consumption, and higher latency.

We analyze how mobility impacts reliability of TSCH protocol in terms of synchronization, message overhead, latency, and energy. The evaluation is performed through simulation and the results show that mobility may cause significant network downtime where nodes are unable to associate to the network for long period of time because of synchronization loss, especially if the network space is not fully covered by static nodes. Association and disassociation issues, induced by mobility, cause frequent disruptions in the network. As per our analysis, although, TSCH can handle mobility if the network space in which mobile nodes are evolving is fully covered by static nodes or there are enough mobile nodes to maintain a consistent coverage. However, the amount of message overhead to maintain synchronization is higher which impacts the reliability of the protocol in terms of energy and latency. Since, most of studies mainly undertake static nodes when using TSCH in several deployments, however, the evaluation of TSCH under mobility is an interesting case that takes into account wireless connectivity together with mobility to offer potential benefits.

7.2 Related Work

In this section, we present related work that studied TSCH under node mobility. The impact of node mobility on TSCH protocol is studied in [186], where authors show how mobility causes disruptions in network and effects network performance. In this work, the focus is on comparison between TSCH and LLDN protocols. Particularly, the process of network association and disassociation incur signaling overhead for scanning the EBs which is costly for resynchronization attempts and energy. The signaling cost gets higher when multiple channels have to be scanned for longer time to rejoin the network causing not only more energy consumption but also increased latency. The evaluation is performed through simulation and authors reveal that synchronization issues can be mitigated by proper beacon and timeslot scheduling schemes. They argued that scanning on a single channel leads to low scanning time for network association thus saving on energy and latency.

The above work mainly undertakes the EBs scanning process into account which leads to more energy consumption and higher latency in the presence of mobile nodes. Whereas, our work focuses more on synchronization issues and we show that the mobile nodes do not consume more power and TSCH can handle mobility well if the network space is fully covered by the mobile nodes.

The same authors have developed the mobility-aware framework in [187] called Mobile TSCH (MTSCH) which facilitates network association process for mobile nodes and reduces latency. The framework used passive beacons instead of EBs to advertise the network. These passive beacons make use of ACK messages to be transmitted on a fixed channel by the network coordinator to advertise the network for other nodes. In this way, nodes only scan on a fixed channel rather scanning all available channels thus it conserves energy and reduces latency to receive synchronization messages to join the network compared to default TSCH. The framework was evaluated through simulation and the results revealed that MTSCH was able to decrease the radio duty cycle of the mobile nodes by 7% to 50% on average and it increased network joining time of the nodes by 3% to 50%.

7.3 Simulation and Experimental Setup

In this section, we first describe the approach that explains the metrics considered. Subsequently, we present the experimental setup and the associated simulation environment.

7.3.1 Approach

We study synchronization (see Chapter 4) issues occurring in a mobile TSCH network. Especially, the issues pertain to frequent disassociation from the network due to mobility and attempting to resynchronize to the network so as to associate with it. In this regard, we analyze:

- **Downtime**: It is the percentage of time a node is out of the TSCH network. This is because mobile node cannot receive EBs, therefore cannot synchronize to the network and hence cannot communicate.

- **Energy consumption**: The energy consumption of the radio devices is calculated based on the assumption that a normal TSCH timeslot, either transmit or receive, consumes 12 mA in average and an idle slot consumes 0.4 mA [181]. Since only the synchronization process is considered, the energy consumption will increase if an application is using the TSCH network.

- **Number of Keep-Alive sent**: The KA messages are unicast messages sent, besides EBs, to prevent the node to desynchronize from the network. The number of KA messages sent shows how close a node is to desynchronize.
  KA messages are sent when there is no traffic in the network and nodes want to synchronize. Thus, it is possible to incorporate the time information elements

on data packet, thus reducing the number of KA messages when data is flowing through the network.

In case of an static network with all nodes inter-connected, the downtime is expected to be 0%. However, mobile nodes resynchronize often with different neighbors. Even in a network space fully covered with TSCH nodes, this resynchronization process sometimes makes the nodes disconnect and reconnect quickly thus causing the downtime to increase. Since a node with a high downtime can neither transmit nor receive any packet, this metric is critical and must be minimum to ensure a reliable performance of the network. We decided to test exclusively MAC layer metrics and not application layer metrics because we noticed that the routing layer choice had the most impact on the application layer performance. However, these results are applicable to the application layer assuming no routing is used.

7.3.2 Experimental Setup

The evaluations are performed through simulation with the Cooja emulator tool. We generate the mobility for the nodes with the mobility framework[1] available for Cooja. Cooja emulates real nodes and guarantees the behavior and characteristics similar to reality.

A TSCH node requires to receive an EB from a neighbor node to be able to synchronize and join the network. To do so, all schedulers rely on a common shared slot among all nodes. To this extent, the IETF provides a minimal TSCH (*TSCH_min*) slotframe [145], which is a basic slotframe that defines an schedule having only one shared slot. In our experiments, we use the minimal TSCH slotframe to analyze the synchronization among all nodes. We configure the slotframe with the recommended parameters having the length of 11 timeslots and a timeslot duration of 10 ms. The EB period is 16 seconds, meaning that a synchronized node emits an EB at least once every 16 seconds. Other schedulers may have different ways of initiating the synchronization process. For instance, the Orchestra [188] relies on the routing protocol RPL to schedule the EB slotframe. However, for RPL to know which neighbor nodes are in range, it relies on a slotframe identical to minimal TSCH, with a size of 31 timeslots. Therefore, our analysis on the minimal slotframe does cover these cases. All the simulation parameters are summarized in Table 7.1. We restrict the field size to 100 meter

[1] http://anrg.usc.edu/contiki/index.php/Mobility_of_Nodes_in_Cooja

Table 7.1: Simulation parameters

Parameter	Value
Field size	100 m × 100 m
Transmission range	100 m
Reception range	50 m (with distance loss)
Network	Mobile
Mobility speed	0 to 4 $m\,s^{-1}$
Mobility model	Random Walk model
Number of nodes	Variable {5 and 10}
Slotframe length	11 timeslots
Slot duration	10 ms
Transceiver	CC2420
Frequency spectrum	2.4 GHz
Propagation model	Two-ray ground model

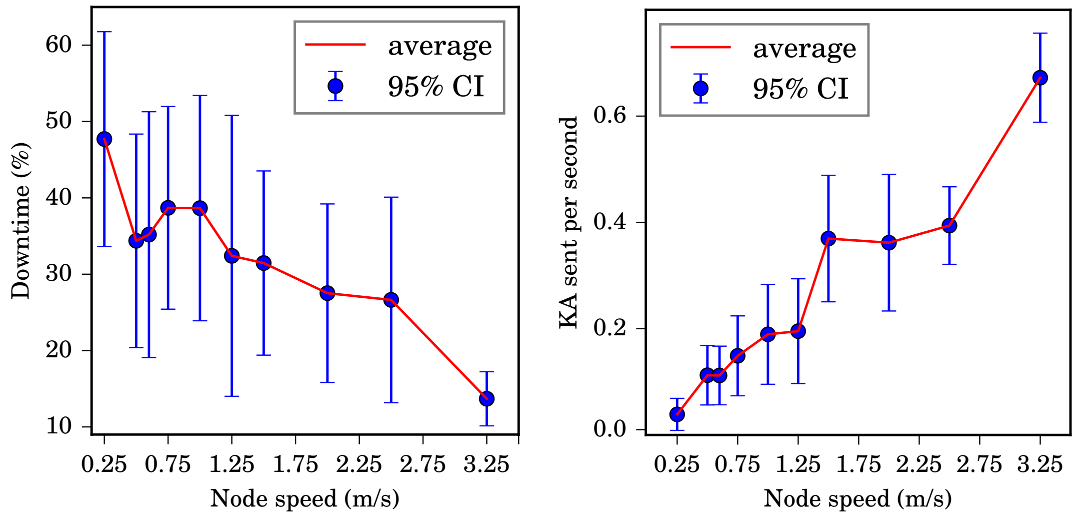
× 100 meter as it corresponds to the size of an industrial area where TSCH nodes are likely to be used. Here, a node covers 19.6% to 78.4% of the field in reception range depending on it's position. The transmission range of 1 node covers 78.4% to 100% of the field depending on its position. In our experiments, external perturbations are not considered, this means that the results obtained are the representative of the best-case (ideal) scenario. In all the experiments, the initial placement of the nodes is random. To gather accurate results, the tests are run between 10 and 30 times and the average metric is presented (in red), with the 95% confidence interval (CI) (in blue) to be discussed in Section 7.4. This means that 95% of all tests performed fall within this interval.

7.4 Evaluation Results and Discussions

In this section, we discuss the results which takes into account the speed of the nodes, varying number of mobile nodes, and the space covered. In particular, we focus on the behavior and synchronization issues of a TSCH network by considering the above parameters.

7.4.1 Speed

First we analyze the effects of one mobile node's speed in a small three-nodes TSCH network. The mobile node follows a random walk model [189] in the restricted space of size 100 meter ×100 meter. In our model, we consider four possible steps (north, south, east, and west) each with the same distance s. One step is taken per second, therefore s is also the speed in meter per second. In this experiment, the nodes cover a reception area from 20.31% to 99.39% of the field depending on their position. Transmission-wise, the coverage is comprised between 79.66% and 100% of the field. The results of this small proof of concept experiment are shown in Figure 7.1. We can see in Figure 7.1a that the downtime is decreasing as the speed of the mobile node increases, and the 95% confidence interval is shrinking, meaning that the downtime is less impacted by the random initial placement of the nodes.



a) Average downtime of all nodes in the network.

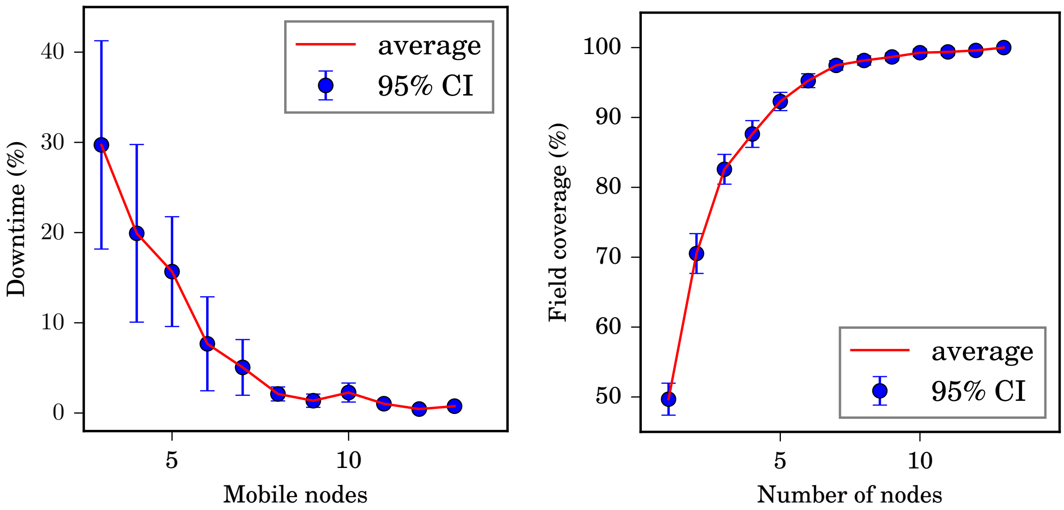
b) Average number of KA messages sent per second.

Figure 7.1: Two static nodes and one mobile node with variable speed.

In Figure 7.1b, we can see that the number of KA messages increases greatly as the speed of mobile nodes increases.

A mobile node with a speed close to 0 behaves similar to an static node. This means that if the mobile node is out of reach of the other nodes, it is not able to join the network quickly. On the contrary, if the mobile node has a very high speed, it is never out of the network which means it desynchronizes but resynchronizes very fast to the next parent node. This causes more KA messages to be sent to maintain synchronization which may impact the network performance by inducing delay and message overhead. However, this may not be the case if the time information element of TSCH is conveyed through data and if data is flowing through all nodes of the network.

7.4.2 Number of Mobile Nodes



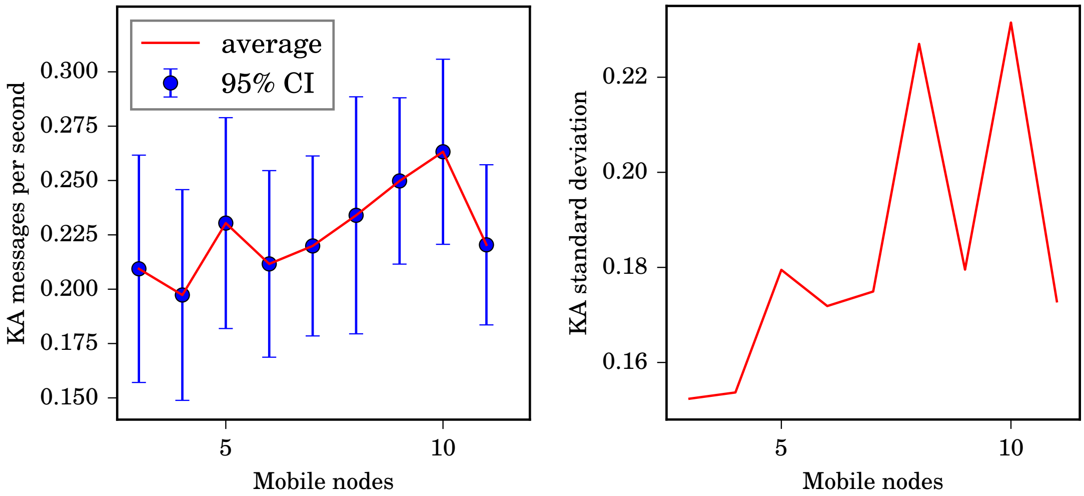
a) Average downtime of all nodes in the network.

b) Field coverage evaluation of the mobile nodes.

Figure 7.2: Downtime analysis when all nodes are mobile.

In the second experiment, we analyze the behavior of the TSCH network when all nodes are mobile and the number of nodes increases. The speed of the nodes is set to $1m/s$. We analyze the downtime and the number of KA messages sent between 3 to 13 mobile nodes.

The results are presented in Figure 7.2 and Figure 7.3. From the downtime analysis, it appears that the average downtime and its standard deviation decrease when the number of mobile nodes increases as shown in Figure 7.2a. This can be related to the nodes' coverage area of the field, as shown in Figure 7.2b. Indeed, as all nodes move in a restricted space, increasing the number of mobile nodes also increases the coverage and thus the probability of each node to be in range of the network. In the 100 meter $\times$ 100 meter space, we see that after 10 nodes



a) Average number of KA sent per second and per node.

b) Standard deviation of the average number of KA sent.

Figure 7.3: KA messages analysis when all nodes are mobile.

the downtime is minimum which is also the number of nodes for which we reach almost 100% coverage in average.

The KA messages analysis shows that a very low number of KA messages are sent per second and the standard deviation is also low as shown in Figure 7.3. More interestingly, it seems that these numbers are not impacted by the number of mobile nodes. Indeed, since all nodes have the same speed there is no difference if there is one or many mobile nodes, the network topology will change at the same speed. Since KA messages are sent to keep being synchronized with the TSCH parent, it is directly related to the network topology. Therefore, the required number of KA messages sent, to keep the network synchronized, stays the same regardless of the number of mobile nodes.

7.4.3 In a Covered Space

In this last experiment, we consider the field space of 100 meter × 100 meter which is covered by 4 nodes and they are placed in the coordinates (30,30), (30,70), (70,70), and (70,30) as depicted in Figure 7.4. With a transmission range of 50 meter, the entire space is covered by these 4 static nodes. This is typically the case of an industrial deployment where robots are moving and static gateways are ensuring stable communication. The number of mobile nodes varies from 1 to 3

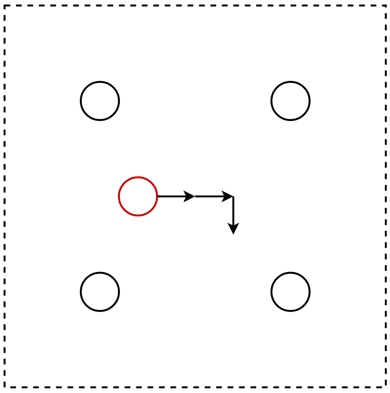
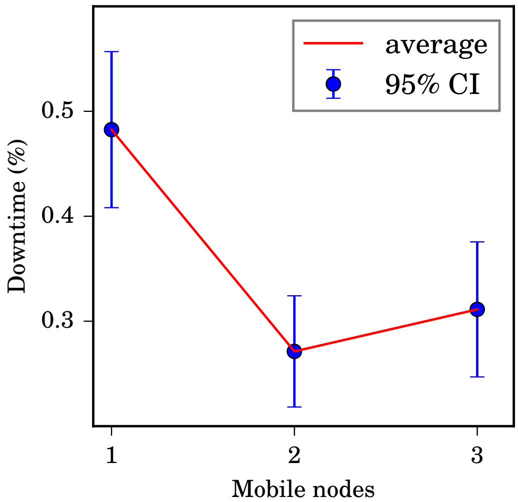
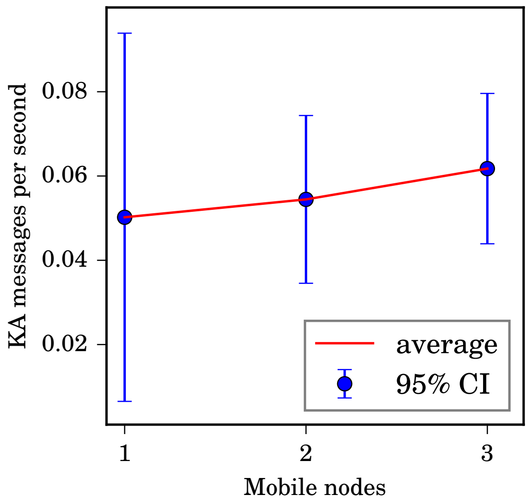


Figure 7.4: Representation of the space covered with one mobile node (in red) and four statc nodes (in black).



a) Average downtime analysis.



b) KA messages analysis.

Figure 7.5: Result of the covered space experiment.

nodes.

The results presented in Figure 7.5a and Figure 7.5b show that regardless of the number of mobile nodes, the downtime is very low with less than 0.5% downtime. The average number of KA messages sent per second and per device is also very low within average 0.05 messages sent. This shows that in a fully covered environment, one or many nodes moving in this space will have no impact on the TSCH network performance and synchronization.

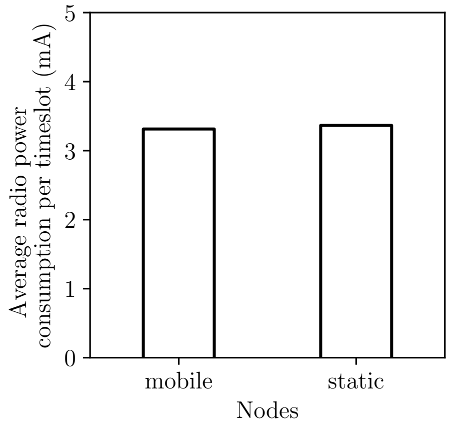


Figure 7.6: Energy consumption comparison in mA per timeslot of mobile and static nodes.

7.4.4 Energy Consumption

To evaluate if a mobile node is consuming more energy, the energy consumption of all nodes was analyzed in a scenario with 5 nodes. In this scenario, some nodes are mobile and others are static. The number of mobile nodes varies from 0 to 5. The results are depicted in Figure 7.6. It appears that there is no difference in energy consumption when the nodes are mobile or static.

Since the movement and placement of these nodes are random, at each time, an static node has the same probability of being disconnected from a mobile node than a mobile node being disconnected from an static node. Another way to see this, is to consider that from the point of view of mobile nodes, the static nodes are moving. Therefore, their energy consumption is similar with $3.3mA$ per timeslot in average.

7.5 Conclusions

This chapter studied TSCH under node mobility. By analyzing the behavior of TSCH with variable node speed, it appeared that having fast mobile nodes decreased the downtime of the network and ensured that all nodes can communicate to one an other. However, it significantly increased the number of KA messages sent and thus overloaded the network, impacting energy and latency. When all nodes were mobile, the results showed that once the network space was fully covered, mobile nodes behaved similarly to an static network; the downtime was close to 0 and the number of KA messages was stable, proportional to the speed of the nodes. Finally, we analyzed the behavior of TSCH in a fully covered space, a typical industrial deployment where mobile robots were evolving and static gateways were ensuring reliable communication. In this scenario, the number of mobile nodes showed no major impact on the network performance. Overall, the energy consumption of a mobile node was same as of an static node.

Our experimental results showed that a TSCH network encountered little synchronization problems if the space where the mobile nodes were evolving was fully covered by static nodes, or if there were enough mobile nodes to guarantee consistent coverage. Therefore, using TSCH mobile nodes together with static nodes, which fully cover the network environment, will ensure a healthy network behavior.

CHAPTER 8

Dual-Mode Time-Slotted MAC Protocol

THIS chapter is dedicated towards the design and evaluation of the Dual-Mode Time-Slotted-Medium Access Control (DMTS-MAC) protocol. DMTS-MAC targets industrial process control applications under IWSAN and it aims to satisfy constraints such as reliability, low latency, scalability, and energy.

We provide a brief background overview of specific application of the proposed protocol in Section 8.1. Limitations of existing protocols that target similar applications are presented in Section 8.2. We detail the dynamics of the control applications and present a use case of networked control system in Section 8.3. The working of the protocol and its superframe structure and switching aspects are given in Section 8.4. The simulation topology, schedule, and superframe slot calculations are discussed in Section 8.5. The evaluation of DMTS-MAC and the simulation results are presented in Section 8.6 and finally conclusions are drawn in Section 8.7.

8.1 Overview

We focus on Dual-Mode Adaptive-MAC (DMA-MAC) [140] and TSCH protocols as the main motivation and propose the DMTS-MAC protocol for process control applications. DMTS-MAC is based on time-slotted structure together with channel hopping and operates in dual-mode having two superframes, transient and steady. The protocol takes into account the dynamics of process control system and is adaptive to its transient and steady states and it effectively satisfies their traffic requirements. The steady superframe takes care of the high data rate state whereas the transient superframe handles the low data rate state. Thus, enabling service differentiation where resources are available as per the demand of control system.

DMTS-MAC improves upon reliability, scalability, energy, and reduces latency compared to its predecessor DMA-MAC protocol. We compare DMTS-MAC protocol with TSCH due to multi-channel operation since DMA-MAC is a single channel protocol. However, we clearly show the improvements of DMTS over DMA-MAC schematically in Section 8.4. In comparison to TSCH, the most promising capability of DMTS is its intrinsic traffic adaptivity through dual-mode. Our results show that dual-mode protocol performs better in terms of latency and energy compared to TSCH MAC protocol.

8.2 Limitations of Existing Protocols

DMTS protocol is influenced by the emergence of low-power standards such as WirelessHART, TSCH, and recently developed non-standard protocols like GinMAC and DMA-MAC. TSCH is considered a suitable protocol for industrial applications [111], however it is not optimized for the dynamics of process control applications. It does not define how to build and maintain a reliable communication schedule which is mandatory for a time-slotted protocol.

GinMAC and DMA-MAC were proposed to meet real-time constraints of process monitoring systems. GinMAC is characterized by features such as *offline dimensioning*, *Exclusive TDMA*, and *Delay conform reliability control*. Whereas, DMA-MAC offers reliability, predictability, and energy efficiency. It uses TDMA superframe with exclusive timeslots. It deals with two states of process control systems: transient and steady. It switches between the two superframes namely transient superframe and steady superframe and adaptively meets their traffic requirements. The major drawbacks of GinMAC and DMA-MAC are scalability and protection against interference. They do not employ any channel hopping to mitigate interference and fading which makes them less reliable to be used in harsh industrial environments. Both protocols employ retransmission mechanism to compensate for packet loss at the expense of increased delay and energy. Packet loss can be frequent in case of severe interference from other co-located networks and only a single retransmission slot per sensor node cannot efficiently compensate such a loss. Both protocols are limited to 25 nodes which makes them limited to be used in dense industrial applications.

DMTS drives basic characteristics from DMA-MAC except that it does not use retransmission slots within superframe to cope with transmission failures rather it uses channel hopping for it and also maintains synchronization procedure.

Other protocols, for example Z-MAC [87] which utilizes CSMA for low contention and switches to TDMA under high contention. Unlike Z-MAC, DMTS is pure TDMA and implements offline scheduling which means the whole timeslot allocation is preplanned like GinMAC and DMA-MAC.

WirelessHART is the first open industrial standard for process monitoring applications. It uses TSMP protocol which mainly takes care of time synchronization. Network manager is the core element which takes care of slot allocation and routing. WirelessHART is more of a framework which can combine different protocols to handle different functions. DMTS-MAC can be used as a MAC protocol within WirelessHART.

In comparison with TSCH, DMTS uses channel hopping like TSCH but operates in dual-mode. TSCH uses shared and dedicated timeslots within the slotframe, nodes in shared timeslots compete for channel access and can encounter collisions for which a CSMA/CA backoff policy is used, but it makes latency nondeterministic. It employs retransmission capability to cope with transmission failure. On the other hand, DMTS does not use shared slots rather it uses dedicated slots to achieve deterministic performance. Unlike TSCH, it does not use retransmission slots because retransmission of old data is generally not desirable for control applications [43]. In this way, DMTS accommodates more nodes in place of retransmission slots thus improves scalability and reduces latency equal to retransmission slots. For a fair comparison, we restrict TSCH to be only pure TDMA to compare it with DMTS, but the retransmission mechanism is kept intact.

8.3 Process Control Traffic Dynamics

In order to develop any MAC protocol, it is imperative to characterize the traffic they have to handle. We consider two important states of process control systems: 1. transient state 2. steady state. A process controller inherently exhibits transient response and steady state response during its operation and generates different traffic in both states. In beginning, when the control system is initialized, it inherently encounters transient state in which the system is said to be unstable and the values of process variables such as pressure, temperature, etc., vary rapidly. After a certain time called *settling time*, system turns into steady state and is said to be stable. During steady state, process variables values are stable and generate low to moderate traffic.

8.3.1 Essential Features of Dual-Mode Time-Slotted-MAC

Reliable, deterministic, and predictable performance: DMTS achieves reliability by utilizing frequency hopping and determinism through TDMA. We define Reliability R as a function of packet reception rate (ρ), which is the ratio of number of packets received at the sink to the total number of packets generated by the nodes in a time interval T.

$$\rho = \frac{\sum Pkt_{received}}{\sum Pkt_{generated}}$$

The sink constantly calculates the value of ρ, if it gets below a threshold (e.g. 90%) the network is treated as unreliable, else reliable.
Low latency: With the use of time-slotted slotframe structure, latency is deterministic and bounded. We reduce further latency by not allowing nodes to retransmit the same data, which causes delay for the fresh data available to be transmitted immediately.
Throughput: DMTS can achieve high throughput due to multi-channels which increases throughput proportionally to the number of available channels.
Scalability: DMTS is scalable due to multi-channel operation. Further scalability is enhanced by accommodating more nodes in place of retransmission slots in the superframe as to be discussed in Section 8.4.
Energy efficiency: DMTS conserves energy with duty cycling, where nodes turn off radio to save energy. Further, time-slotted access ensures no collision and saves energy. We save further on energy by not allowing nodes to retransmit old data by having retransmission opportunities.
Disadvantages: DMTS-MAC is complex due to dual-mode. The switch between the superframes based on threshold detection is a bit critical and needs to be properly ensured. Use of multi-channels also adds complexity.

8.3.2 Networked Control System Use Case

We consider an Networked Control System (NCS) scenario similar to scenarios in [76] and [140], as shown in Figure 8.1. It depicts a chemical plant which consists of different sensors like temperature, pressure, flow, etc., and actuators (pump, valve). The purpose of the plant is to supervise mixing operation of the two chemicals, contained in Tank1 and Tank2, during mixing in the reaction vessel. The system uses feedback loop to continuously monitor and control the mixing operation through measuring process variables like temperature, pressure, flow, and level. Based on measurements, controller makes decisions and actuators perform necessary adjustments to control process variables.

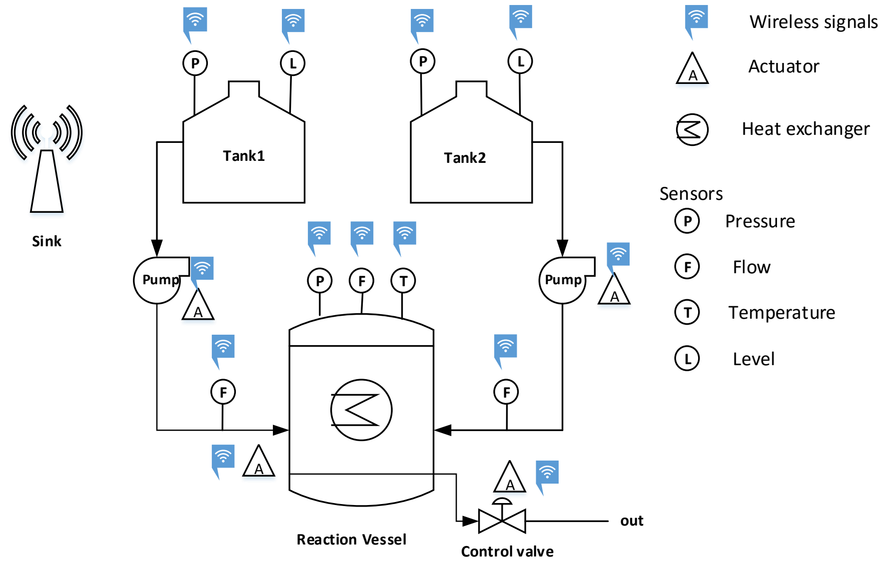


Figure 8.1: A chemical plant with closed-loop control consisting of sensors, controller, and actuators to control the mixing operation.

Mixing operation starts by allowing the chemicals to flow into the vessel, at this point of time, measurement of flow is important. As soon as the flow is complete, chemical reaction starts during which it is important to continuously monitor and control temperature and pressure so that their values are under desired range. Heat exchangers serve as actuators that control temperature in the reaction vessel. As the reaction starts, having flow constant, there is high rate of change of temperature, this shows transient state. After sometimes, the temperature becomes stable and the rate of change of temperature is low, this shows steady state. The corresponding control graph in Figure 8.2 depicts process dynamics [37].

8.4 Dual-Mode Time-Slotted-MAC Working

DMTS-MAC consists of transient superframe and steady superframe. The former essentially requires sensors to frequently transmit data to meet the high traffic demand of process controller, whereas the latter has low to moderate traffic needs which allows sensors to transmit data less frequently and achieve

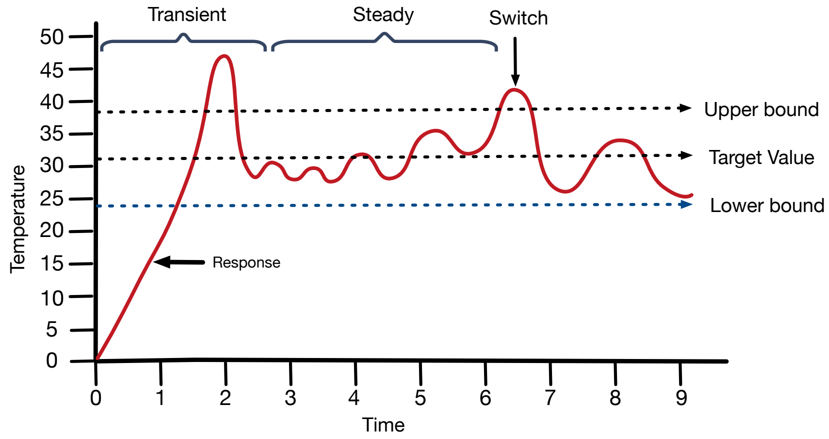


Figure 8.2: Process control states showing transient and steady response.

duty cycling. We propose DMTS for control systems where steady state is more dominant than transient state. Moreover, the process is said to be in transient state continuously until the measurements of process variables turn into the slowest state in steady. One of the important features of DMTS is switching between the two superframes. There are two switch operations involved: (i) transient to steady (ii) steady to transient.

The switch from transient to steady is normally determined by the sink once the process starts to turn into steady and the sink informs all the nodes about this change in the configuration slot. Whereas the change from steady to transient is detected by sensors and sensors inform the sink of this change during the update period. We employ a threshold mechanism to differentiate between the two states. For instance, when measurements of process variables in steady state, detected by sensors, go above some threshold value, sensors will inform the sink of necessary change of the superframe and the sink will take necessary measures to switch to transient state. We assume that the threshold settings for detection of the change of switch between the states is purely a process model phenomenon under consideration.

We define two superframes corresponding to each of the controller states, transient superframe (T) and steady superframe (S) as shown in Figure 8.3 and Figure 8.4 respectively. The reason to use two superframes is to adaptively make valuable communication resources available when needed in times of peak demand and save them in times of low demand. We incorporate different fixed periods consisting of exclusive TDMA slots in each superframe structure as detailed below.

8.4.1 Transient Superframe (T)

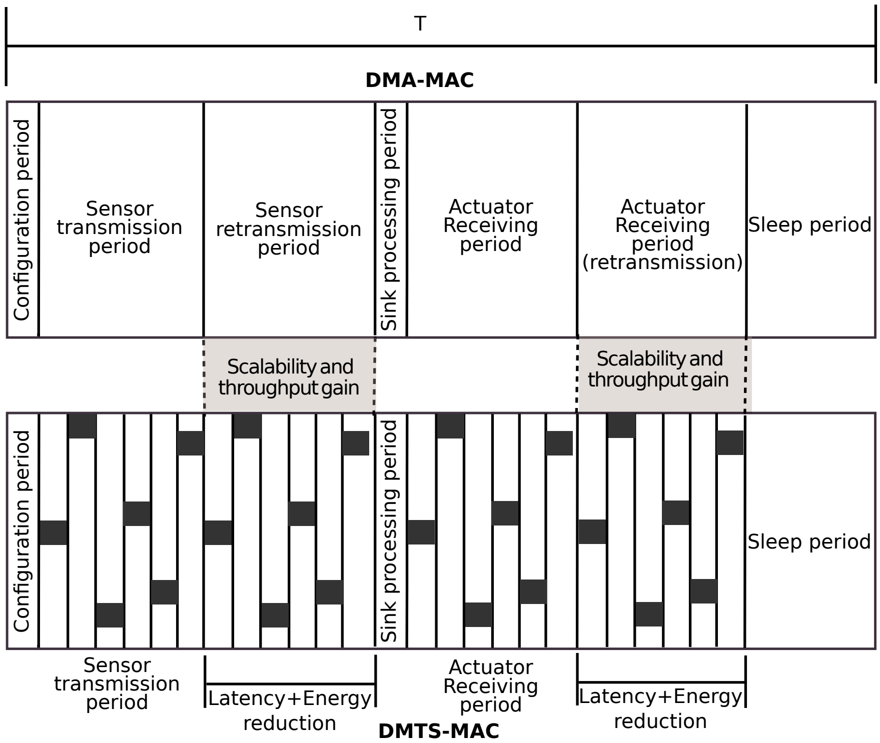


Figure 8.3: Transient superframe showing dedicated timeslots with channel hopping a black square indicates a different channel used in different timeslots.

This superframe uses time-slotted access with channel hopping (Figure 8.3). Every transmission occurs on a different channel. As can be seen, DMTS transient superframe differs from DMA-MAC superframe because it accommodates more nodes in place of existing retransmission slots and uses channel hopping. Thus, it improves reliability, scalability, throughput, and reduces latency and energy consumption. The superframe comprises of following periods appearing alternatively over superframe cycle.

Configuration period: It indicates start of the superframe, and it is used by the sink to broadcast superframe information. This information includes updates of switch from transient to steady and vice versa, frequency hopping sequence, and synchronization information.

Sensor transmit period: It allows sensor nodes to transmit data through exclusive timeslots allocated to them.

Sink process period: It is required by the sink to get control command which is

processed by the controller.
Actuator period: Includes TDMA receiving timeslots for the actuators to receive the control command from sink. This period utilizes channel hopping for high reliability.
Sleep period: Used for duty cycling that allows nodes to sleep by turning off their transceivers to conserve energy.

8.4.2 Steady Superframe (S)

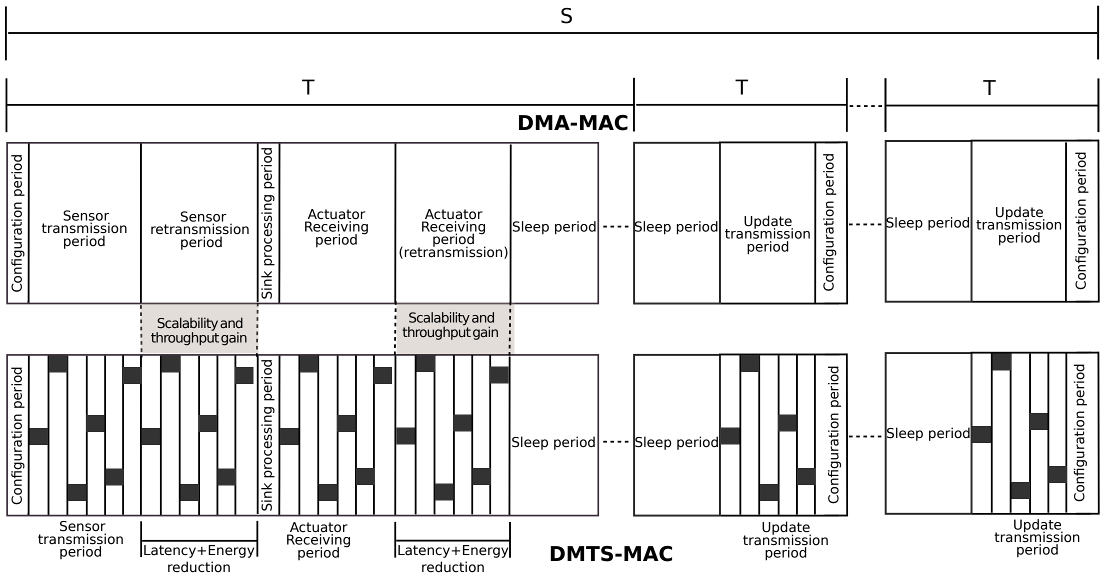


Figure 8.4: Steady superframe showing dedicated timeslots with channel hopping, a black square indicates a different channel used in different timeslot.

The steady superframe (S) meets the requirements of the steady state of process controller. It includes TDMA periods with channel hopping similar to transient superframe (T) as shown in Figure 8.4. The only difference is that S is designed to be multiple of T periods, which means the periodicity of steady superframe is multiple of transient superframe (see Section 8.5). Sensor nodes only transmit and actuators receive during the first T period and sleep and wakeup (only sensors) during the next T periods. Since steady state has low to moderate traffic requirements and this allows nodes to save resources by not transmitting data too frequently when it is not required and hence enables a service differentiation aspect which is common in industrial scenarios. It consists of same periods as transient superframe except update period as described next.

Update period: It is used by sensor nodes only (not actuators) to notify the sink for the change from steady to transient superframe, once they detect the data rate threshold breach. This threshold interval is fixed by the sink. Once sensor nodes realize that the current measurements violates the set threshold, they trigger the update and transmit this information using dedicated update slots.

After the first T period, we repeat configuration period and update period in subsequent T periods in the steady superframe similar to DMA-MAC.

8.4.3 Switching Between Superframes

As already described, the change from transient to steady is imposed and invoked by the sink based on the data it receives from sensor nodes which helps the sink to determine steady state threshold. The sink then makes necessary processing to switch from transient to steady superframe and notifies all sensors and actuators during configuration period. Whereas the switch from steady to transient is detected by sensors based on data rate threshold set by the process model and is critical. In this, sensors notify the sink for state change during the update period once they detect data rate threshold breach.

8.5 Topology and Superframe Schedule

DMTS-MAC is based on a tree topology as shown in Figure 8.5 and the same is used for simulation. This topology is considered to evaluate key aspects of protocol, particularly the multi-hop capability and update data transmission anywhere within topology. Due to space limitation, Figure 8.5 shows partial depiction of topology. It accommodates total of 51 nodes: 38 sensors, 12 actuators, and one

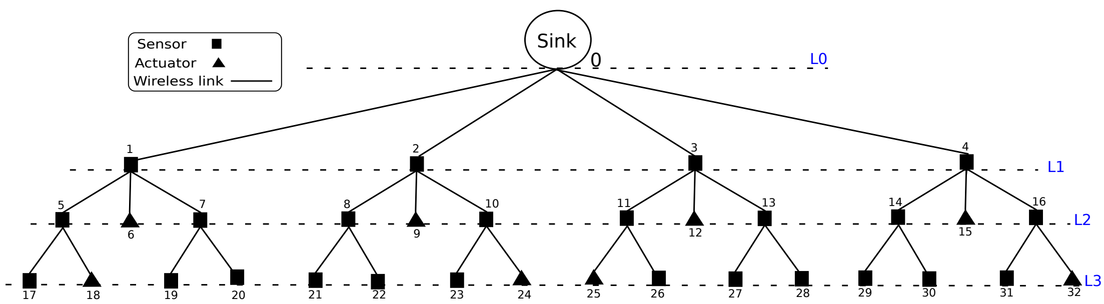


Figure 8.5: Logical network topology for the simulation of DMTS-MAC protocol.

sink. The sink is assumed to be wire connected and has high computational and

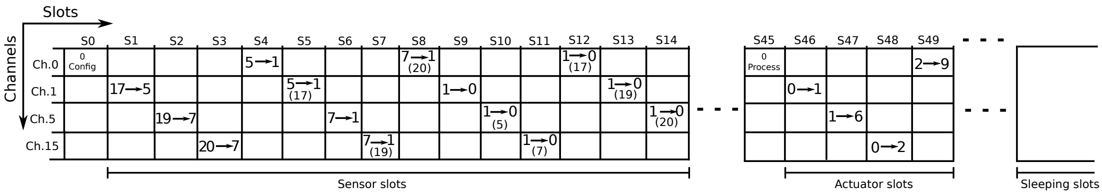


Figure 8.6: DMTS-MAC schedule for sensor and actuator nodes for a part of tree topology of Figure 8.5. The arrow shows the communication flow from the sender to the receiver. The number in the parenthesis below shows the child node whose data the parent node forwards.

transmission power to manage the overall network. The numbers in Figure 8.5 refer to node number in the tree. The letter L prefixed with number represents different levels within the topology. $L0$ represents the level where the sink resides, $L1$ represents the level where nodes reside one hop away from the sink, $L2$ two hops away and so on.

8.5.1 Scheduling and Channel Hopping

Figure 8.6 depicts a part of the communication schedule based on Figure 8.5 for DMTS-MAC implementation. We use CC2420 transceiver, thus, 16 channels are available to hop through. Every timeslot uses different channel and achieves resilience. Only one transmission is scheduled on each channel in a timeslot to limit interference due to concurrent transmissions so that transmission failures are avoided, this enhances reliability. The schedule is computed offline and it is given as input through XML files to the OMNeT++ simulation similar to DMA-MAC implementation. The difference in the DMTS-MAC schedule compared to DMA-MAC is the use of multi-channels.

8.5.2 Superframe Timeslots Calculations

The network topology in Figure 8.5 can be seen as a tree $G = (V, E)$, where V is the set of k nodes and E is the set of $k - 1$ edges called links among the nodes. There are different types of nodes in the tree. One is the sink node r, a set of sensor nodes N and a set of actuator nodes A, such that $V = \{r\} \cup N \cup A$. For an actuator node $a \in A$ there exists exactly one edge $(w, a) \in E$, with $w \in N \cup \{r\}$. The distance $d(v, u)$ is the number of edges between $v, u \in V$. The level $l(v) = d(v, r)$ is the number of edges between $v \in V$ and the sink r.

Transient Superframe Timeslots

The total duration of the transient superframe is T that consists of different timeslots in the respective periods and is calculated as:

$$T = (2 + e + f) \times \eta + t$$

Here 2 represents the one timeslot for configuration and one for sink processing periods, e denotes sum of the timeslots required for senors to transmit information to the sink based on multi-hop distance at each level in the tree. Similarly f denotes the sum of the timeslots required for actuators to receive command from the sink based on multi-hop distance at each level. Both e and f are calculated as:

$$e = \sum_{n \epsilon N} l(n) \quad , \quad f = \sum_{a \epsilon A} l(a)$$

The η is the duration of the timeslot which is 10 ms and t denotes sleeping timeslots.

Steady Superframe Timeslots

Since, steady superframe is multiple of transient superframes, so the total number of timeslots in steady superframe (S) depends on the number of transient parts (m) so; $S = m \times T$. In both superframes, whole timeslot is used to send a maximum size packet p. Thus total bandwidth required is p per superframe (S or T).

8.5.3 Maintaining Synchronization

Synchronization is maintained through notification transmitted in configuration period. Notification message resets the timeslot counter to 0 on every transmission regardless of the state of the nodes. The nodes simply use the time of configuration slot (x), slot duration (η), and the number of timeslots passed (z) since the beginning of the superframe as follows: $Sync = x + (\eta \times z)$. Thus, the configuration message serves to overcome loss of synchronization.

8.6 Performance Evaluation and Results

We evaluate DMTS-MAC in OMNeT++ [173] simulation environment together with INETMANET framework [177] as a supporting platform for our implementation. The whole implementation of DMTS-MAC is done in C++ that is inherited from the MACProtocolBase which is part of INETMANET library. The network and application layers have been used from INETMANET framework. The evaluation is based on frame distribution, which is actually the ratio of transient superframe to steady superframe similar to DMA-MAC implementation. This ratio, in principle, determines the ratio between transient states and steady states of network during simulation.

8.6.1 Configurations

Table 8.1: Simulation parameters

Layer	Parameters	Value
APP	Field size	250 m x 250 m
	Network	Static
	Number of nodes	51
	Simulation time	1350 s
	Data packet size	44 Bytes
MAC	Slot duration	10 ms
	Transient superframe length	1.5 s
	State switch probability	0.1, 0.5
	Number of rounds	900
	Data packet size	44 Bytes
	ACK, update alert packet size	11 Bytes
PHY	Transceiver	CC2420
	Frequency spectrum	2.4 GHz
	Propagation model	Two-ray model

Three main configurations are used for simulation based on different probabilities of transient superframe appearing in a given duration of time. For example, transient superframe appears with probability p and steady superframe appears with probability $1-p$. We present transient superframe appearing with probability $p = 0.1$, $p = 0.5$, and $p = 1.0$. The probability $p = 1.0$ represents TSCH whereas the others represent DMTS. The protocol switches between two superframes based on this probability. The $p = 0.1$ probability represents processes in which steady state is more dominant and are more stable. Whereas $p = 0.5$ shows processes which are less stable and transient superframes appear more frequent to handle high traffic load of transient state.

We also consider update probability where nodes request the change of superframe from steady to transient, if they detect the data rate threshold breach. Please note that the state switch probability of the sink is different from the update probability of the sensor nodes. State switch probability is one with which the sink changes from transient to steady based on the process model, whereas the update probability is used by sensor nodes and not the actuator nodes to generate update switch information if they detect the threshold breach. Thus, they are different probabilities. In order to obtain our desired ratio of 10% and 50% of state switch probability, we achieve the desired update probability that correspond to these ratios by running preliminary simulations again and again.

In all configurations, we use steady superframe twice the length of the transient superframe. DMAMAC was evaluated with total of 900 superframes in a given simulation duration, and therefore, we also measure transient superframes of DMTS-MAC relative to 900 transient superframes for similar simulation duration. Detail of the simulation parameters is listed in Table 8.1.

8.6.2 Noise Generation

INETMANET implements *interference ball model* (IBM) [190] which considers aggregated impacts of near-field interferers. It is based on the additive interference and Signal-to-Interference-and-Noise-Ratio (SINR) thresholding to receive the packets. In this way, from a node perspective, all the rest of transmissions, which are in-progress, are treated as noise when calculating noise level. However, for a certain acceptable Bit Error Rate (BER), the SINR has to exceed an appropriate threshold. The transmit power used by the transmitter of link l denoted as P_l, the SINR perceived by the receiver of link m, denoted by γ_m, is given by [191]:

$$\gamma_m = \frac{Gm_o, m_d \; P_m}{P_{\mathcal{N}} + \sum_{l \in \mathcal{L} \setminus \{m\}} G_{l_o, m_d} \; P_l}$$

where channel gain from the point X to the point Y is denoted by $G_{X,Y}$, l_o represents the transmitter and l_d the receiver of link l, and $P_{\mathcal{N}}$ denotes the thermal noise power in the frequency band of operation. Note that nodes are identified with their locations. The sum in the denominator is taken over all links $l \in \mathcal{L} \setminus \{m\}$ where $\mathcal{L}$ denotes the set of concurrently active links [191].

For simulation, we generate noise on a specific channel by increasing the channel background noise. In this way, channel is more noisy and whenever nodes encounter this channel they are unable to communicate, the noise affects all nodes equally. If nodes encounter noisy channel, they hop to another channel and resume transmission.

8.6.3 Packet Delivery Ratio

PDR determines reliability of the protocol, it can be seen in Table 8.2 that both protocols ensure reliability as they both maintain mean PDR value of more than 90%. However, there is little less PDR in DMTS-MAC which is due to the nodes encountering noisy channel randomly. Since TSCH utilizes retransmission where nodes whose transmission fails can use retransmission opportunity, thus achieves relatively higher PDR. Comparing the two configurations of DMTS-MAC, the $p = 0.5$ configuration involves more number of superframe switches compared to $p = 0.1$, therefore the former has a slightly less PDR than the latter because of noise where nodes are unable to switch to respective superframe as a result of failing to receive switch notification message during configuration period. Overall, both protocols are reliable as they achieve more than 90% PDR.

Table 8.2: PDR comparison

Protocol	Configuration	PDR
DMTS	$p = 0.1$	0.9276
	$p = 0.5$	0.9275
TSCH	$p = 1.0$	0.9999

8.6.4 Latency Analysis

The end-to-end latency of the protocol is determined when the first sensor transmits data and the last actuator receives it. This, in turn, depends on the size of the superframe. The superframe is of static nature for both protocols. Thus maximum delay for transient superframe is 1200 ms for DMTS and 2400 ms for TSCH. DMTS protocol has less latency because of having no retransmission. Although, it is a design choice, TSCH can also disable retransmission and achieve same latency but the protocol is not optimized for control applications. There is always a trade-off between number of timeslots and latency for supeframe-based protocols.

8.6.5 Energy Efficiency

The energy consumption is based on time spent by nodes in transmit, receive, and sleep. The values of current consumption in these states are obtained from

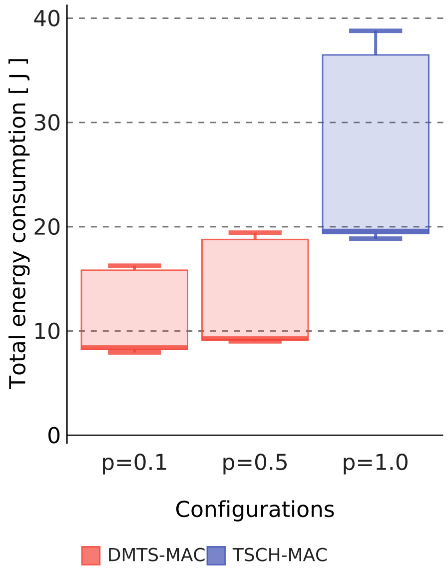


Figure 8.7: Total energy consumption comparison between DMTS-MAC and TSCH under different configurations.

the CC2420 data sheet [192]. The energy consumption across the network is not uniform for all the nodes because of tree topology where nodes near the sink have higher traffic load. Thus, we take into account total energy consumption as the metric to compare DMTS and TSCH. DMTS-MAC consumes less energy in $p = 0.1$ and $p = 0.5$ configurations as shown in Figure 8.7, because the percentage of time nodes are active is lower compared to TSCH. Since, TSCH uses retransmission mechanism so the percentage of time nodes are active is high. Further, TSCH is restricted to single superframe, which does not let it save communication resources in times of low demand and utilize them efficiently in times of high demand. This leads to more energy consumption in TSCH. Comparing both configurations of DMTS, $p = 0.1$ consumes less energy compared to $p = 0.5$, because transient superframe appears more frequent in the former configuration than the later, thus it relatively consumes more energy because transient is more data intensive state.

8.6.6 Failed Switches

Figure 8.8 depicts the number of failed switches on a log scale for both configurations of DMTS-MAC. TSCH is single-mode and does not involve switching, thus no switch failures are depicted. Failed switches happen for two reasons (i) The

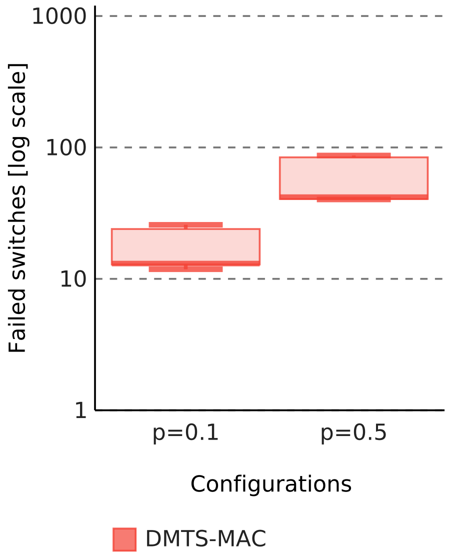


Figure 8.8: Switch failure comparison.

update switch information from the sensor nodes fails to reach the sink due to packet loss or noise and thus renders the sink unable to make superframe switching decisions (ii) The configuration message from the sink that informs the nodes for the suprframe change, can fail to reach the nodes, which causes some of the nodes to continue to operate in steady state. In case of (ii), as steady superframe is multiple of transient superframe therefore, it is possible that some nodes can face delay to switch to the desired operational mode when they fail to receive configuration message for state change due to packet failure. The configuration message contains the information related to the current state, the network is working in. In case a node is not in the desired state as the sink, it can easily synchronize once it receives the configuration message.

Although, channel hopping effectively copes with noise and interference to transmit update switch information, yet there are relatively very less switch failures occurred as a result of node encountering noisy channel randomly. Configuration $p = 0.5$ has relatively more number of switch failures than $p = 0.1$ because the transient state appears more often in it. To ensure more reliability, redundant timeslots may be added to further increase possibility to transmit update information, however it increases energy consumption and delay.

8.7 Conclusions

We proposed DMTS-MAC protocol that targets to satisfy the stringent requirements such as reliability, latency, energy, and scalability of industrial process control applications. The protocol is evaluated for these metrics through simulations with the help of OMNeT++ simulation environment. The protocol is variant of the DMA-MAC, but unlike DMA-MAC superframe, DMTS-MAC superframe introduces more nodes in place of retransmission slots to enhance scalability and exploits channel hopping to achieve reliability against interference similar to TSCH. Further, DMTS-MAC is scalable upto 50 nodes compared to DMA-MAC protocol which is limited to 25 nodes under the same constraints of latency. In comparison to TSCH, DMTS is pure TDMA with two superframes whose dual-mode and adaptive schedule takes care of the varying traffic requirements of transient and steady states of process control applications. The results showed that DMTS-MAC is reliable in terms of PDR, less energy consuming, and accommodates more nodes under the same latency constraints. Although, there were certain switch failures occurred yet the protocol was able to maintain more than 90% of the PDR and consumed less energy compared to TSCH protocol.

CHAPTER 9

Conclusions and Future Outlook

IN this chapter, we draw conclusions on the overall research work that has been presented in this thesis, particularly, main contributions, results, and future directions are put into perspective.

We highlight the contributions in Section 9.1 and present future directions in Section 9.2.

9.1 Conclusions

As IWSANs continue to proliferate in various industrial applications, many challenges such as reliability, low latency, scalability, and energy require satisfactory solutions so as to maintain an acceptable QoS for these applications. Particularly, in the domain of process control which encompasses actuators along with sensors put a great deal of challenge on MAC protocol design. Although, current MAC protocols employ different ways to overcome such challenges yet they still pose threats on the network performance and require enhancements under varying network conditions.

This dissertation first addressed above mentioned challenges and proposed an enhanced MAC protocol which could overcome these challenges. The evaluations of the protocol, through simulation, showed that the protocol offered enhanced performance in terms of reliability, low latency, scalability, and energy efficiency. The main contributions of this thesis can be summarized as follows.

- We provided a comprehensive study of various MAC protocols in general and IWSAN MAC protocols in particular, that target to meet severe requirements of industrial monitoring and control applications. We explored several low-power industrial standards and technologies like IEEE 802.15.4 standard and its derivations such as WirelessHART, ISA100.11a, WIAPA, 6LoWPAN, and 6TiSCH. We determined the suitability of these standards across different industrial applications. Our analysis identified several limitations of existing protocols under various performance metrics such as reliability, latency, scalability, and energy. We emphasized the need to overcome these limitations of the existing standards so as to meet aforementioned performance metrics of industrial applications.

- Various technologies and standards that share common frequency bands, such as ISM, generate severe interference in a coexisting environment. We investigated how the inherent PHY and MAC layer design of these standards and technologies help cope with interference issues and what other techniques can be employed to achieve better performance.

- We investigated the problem of inter-network interference in the context of dense industrial low-power networks which arises with the use of unlicensed bands in a coexisting environment. We analyzed the behavior of TSCH MAC in co-located environment and showed that while the protocol performs well in standalone networks, it poses network reliability problems when operated in close proximity to other TSCH networks. The fact that IoT demands dense deployments of low-power networks for different applications, however these networks employ license-exempted bands and thus they may pose huge interference for one another. Therefore, the performance of MAC protocols should be examined under different network conditions such as number of networks operating in close proximity and the number of nodes in each network. As per our analysis, in case of TSCH protocol, the synchronization sources or clock sources should be chosen carefully to avoid network degradation. Moreover, the use of diverse channels in the network as opposed to fewer channels, performs better in mitigating inter-network interference.

- We provided analysis on the node mobility problem in the context of emerging industrial applications which require mobility to achieve autonomous operation and improve operational efficiency. In this regard, we provided a thorough analysis of TSCH reliability in the presence of mobile nodes. We studied different networks and having different number of static and mobile nodes in each network along with using different speed of the nodes. Our results provided useful insights on the impact of mobility on the reliability of TSCH protocol. We came to the conclusion that TSCH can provide reliable performance if the space in which nodes are operating is fully covered by mobile nodes or there are enough static nodes to guarantee a consistent coverage.

- As a major contribution, we proposed DMTS-MAC protocol that guarantees reliability, low latency, scalability, and energy efficiency. The protocol overcomes the limitations of the existing DMA-MAC and GinMAC protocols by proposing enhanced modifications. The modifications have been extensively evaluated through simulations. The unique feature of the DMTS protocol is that being a pure TDMA, it exploits dual mode capability that involves switching between different TDMA schedules based on the intrinsic properties of the process controller. In this way, it adaptively satisfies the varying traffic requirements of the process control applications. The protocol employs channel diversity to overcome fading and interference of wireless medium and achieves reliability in non-ideal conditions. The duty cycle achieves energy efficiency without compromising on latency and supports more number of nodes.

9.2 Future Directions

Although, the performance of DMTS-MAC is promising under many performance metrics, yet it would be interesting to extend the investigation of protocol with respect to following aspects.

- Given different traffic with diverse criticality of various classes of industrial applications, it would be more beneficial to exploit DMTS-MAC protocol to tackle any kind of traffic based on different priority of the data but then multiple schedule or pre-configured timeslots should be incorporated and investigated.

- The use of update slots is indispensable in the current DMTS-MAC design to trigger the state switch, however, to reserve a bandwidth for an event whose occurrence is unknown and unpredictable is a waste of resources. Therefore, rather dedicating slots in each superframe, the alternative strategies should be sought to save further on energy and latency. This can be further researched in greater insights given the constraints of application on protocol design and the trade-off complexity involved.

- The other interesting direction can be to use the DMTS-MAC protocol in combination with other wireless standards such as WirelessHART and ISA and test its performance.
- Security is another aspect that can be tested in connection with DMTS-MAC protocol. As the WirelessHART, ISA, and other standards employ dedicated security managers, the security features can be embedded in DMTS to make it more secure. Providing a dedicated security manager is costly and impracticable for many small industrial plants, however, building such feature inherently into the protocol will save cost and add flexibility.
- DMTS-MAC encounters switch failures due to interference and noise, it would be worth while to assess the channel first through some link quality estimations to predict the channel condition before making transmission and avoid bad channels. In this way black listing interfering channels will further avoid the probability of switch failures and enhance reliability.
- We tested the TSCH protocol in a co-located scenario through simulations. However, the same can be tested in real-world deployment which depicts a realistic IoT scenario, this will give practical insights on the protocol performance. While the existing trend is to test MAC protocols in standalone network without taking into account the effects of nearby networks, however the practical approach can be to test the protocol by considering the effects of nearby networks and asses its reliability in more depth.
- Inter-network interference can be tested with different scheduling schemes to see which performs better and will give better insights on the protocol performance associated with the given schedule.

Finally, as TSCH MAC protocol serves to be ideal protocol for various IoT and industrial IoT applications, therefore, more experimental studies need to be conducted to determine its true strengths. Moreover, coexistence of networks using unlicensed band is inherently the part of industrial IoT ecosystem, thus protocols must be evaluated not only in standalone networks but also in dense deployments with other networks. In this way, we can determine how efficiently the protocol can cope with the several issues that may cause degradation of several performance metrics like reliability, latency, scalability, and energy.

Bibliography

[1] Aaron S Crandall and Diane J Cook. Smart home in a box: A large scale smart home deployment. In *Intelligent Environments (Workshops)*, pages 169–178, 2012.

[2] C Nay. Sensors remind doctors to wash up. *IBM Res., Armonk, NY, USA*, 2013. https://www.ibm.com/blogs/research/2013/11/sensors-remind-doctors-to-wash-up/, Last visited: 03.05.2019.

[3] Kaarin Michaelsen, Jason L Sanders, Shanta M Zimmer, and Gregory M Bump. Overcoming patient barriers to discussing physician hand hygiene: do patients prefer electronic reminders to other methods? *Infection Control & Hospital Epidemiology*, 34(9):929–934, 2013.

[4] I. Ungurean, N. C. Gaitan, and V. G. Gaitan. An IoT architecture for things from industrial environment. In *Processing of the International Conference on Communications (COMM)*, pages 1–4. IEEE, 2014.

[5] Chengen Wang, Zhuming Bi, and Li Da Xu. IoT and cloud computing in automation of assembly modeling systems. *IEEE Transactions on Industrial Informatics*, 10(2):1426–1434, 2014.

[6] Kusum Dalal and Pawan Dahiya. State-of-the-art in vanets: The core of intelligent transportation system. *IUP Journal of Electrical and Electronics Engineering*, 10(1):27, 2017.

[7] Fernando Camacho, César Cárdenas, and David Muñoz. Emerging technologies and research challenges for intelligent transportation systems: 5G, hetnets, and sdn. *International Journal on Interactive Design and Manufacturing (IJIDeM)*, pages 1–9, 2017.

[8] Jordi Serra, David Pubill, Angelos Antonopoulos, and Christos Verikoukis. Smart HVAC control in IoT: Energy consumption minimization with user comfort constraints. *The Scientific World Journal*, 2014, 2014.

[9] Tomas Gea, Josep Paradells, Mariano Lamarca, and David Roldan. Smart cities as an application of internet of things: Experiences and lessons learnt in barcelona. In *Proceeding of the International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing*, pages 552–557. IEEE, 2013.

[10] Veronica Scuotto, Alberto Ferraris, and Stefano Bresciani. Internet of things: Applications and challenges in smart cities: a case study of ibm smart city projects. *Business Process Management Journal*, 22(2):357–367, 2016.

[11] Fadi Shrouf and Giovanni Miragliotta. Energy management based on Internet of Things: practices and framework for adoption in production management. *Journal of Cleaner Production*, 100:235–246, 2015.

[12] Chin-Feng Lai, Ying-Xun Lai, Laurence Tianruo Yang, and Han-Chieh Chao. Integration of IoT energy management system with appliance and activity recognition. In *Proceeding of the International Conference on Green Computing and Communications (GreenCom)*, pages 66–71. IEEE, 2012.

[13] Zubair Md Fadlullah, Mostafa M Fouda, Nei Kato, Akira Takeuchi, Noboru Iwasaki, and Yousuke Nozaki. Toward intelligent machine-to-machine communications in smart grid. *IEEE Communications Magazine*, 49(4), 2011.

[14] Franck L Lewis et al. Wireless sensor networks. *Smart environments: technologies, protocols, and applications*, pages 11–46, 2004.

[15] D. Porcino and W. Hirt. Ultra-wideband radio technology: Potential and challenges ahead. *IEEE Communications Magazine*, 41(7):66–74, 2003.

[16] Ian F Akyildiz and Ismail H Kasimoglu. Wireless sensor and actor networks: research challenges. *Ad hoc networks*, 2(4):351–367, 2004.

[17] J. Åkerberg, M. Gidlund, and M. Björkman. Future research challenges in wireless sensor and actuator networks targeting industrial automation. In *2011 9th IEEE International Conference on Industrial Informatics*, pages 410–415, July 2011.

[18] Edward A Lee. Cyber physical systems: Design challenges. In *Proceeding of the International Symposium on Object and Component-Oriented Real-Time Distributed Computing (ISORC)*, pages 363–369. IEEE, 2008.

[19] Jay Lee, Behrad Bagheri, and Hung-An Kao. A cyber-physical systems architecture for industry 4.0-based manufacturing systems. *Manufacturing Letters*, 3:18–23, 2015.

[20] Nagesh Nandiraju, Deepti Nandiraju, Lakshimi Santhanam, Bing He, Junfang Wang, and Dharma P Agrawal. Wireless mesh networks: Current challenges and future directions of web-in-the-sky. *IEEE Wireless Communications*, 14(4), 2007.

[21] T. Winter, P. Thubert, A. Brandt, J. Hui, R. Kelsey, P. Levis, K. Pister, R. Struik, JP. Vasseur, and R. Alexander. Rpl: Ipv6 routing protocol for low-power and lossy networks. Internet Requests for Comments, March 2012. `http://www.rfc-editor.org/rfc/rfc6550.txt`.

[22] Heiner Lasi, Peter Fettke, Hans-Georg Kemper, Thomas Feld, and Michael Hoffmann. Industry 4.0. *Business & Information Systems Engineering*, 6(4):239–242, 2014.

[23] IEEE Computer Society. IEEE standard for low-rate wireless networks. *IEEE Std 802.15.4-2015 (Revision of IEEE Std 802.15.4-2011)*, pages 1–709, April 2016.

[24] IEEE standard for information technology - telecommunications and information exchange between systems - local and metropolitan area networks specific requirements part 15.4: Wireless medium access control (mac) and physical layer (phy) specifications for low-rate wireless personal area networks (lr-wpans). *IEEE Std 802.15.4-2003*, pages 01–670, 2003.

[25] IEEE standard for information technology– local and metropolitan area networks– specific requirements– part 15.4: Wireless medium access control (mac) and physical layer (phy) specifications for low rate wireless personal area networks (wpans). *IEEE Std 802.15.4-2006 (Revision of IEEE Std 802.15.4-2003)*, pages 1–320, Sept 2006.

[26] IEEE Standard. IEEE standard for local and metropolitan area networks– part 15.4: Low-rate wireless personal area networks (lr-wpans) amendment

1: Mac sublayer. *IEEE Std 802.15.4e-2012 (Amendment to IEEE Std 802.15.4-2011)*, pages 1–225, April 2012.

[27] ZigBee Alliance. `http://www.zigbee.org/`, Last visited: 02.04.2019.

[28] WirelessHART. `https://fieldcommgroup.org`. Last visited: 14.04.2019.

[29] The international society of automation- isa. `https://www.isa.org/`. Last visited: 28.04.2019.

[30] N. Kushalnagar, G. Montenegro, and C. Schumacher. Ipv6 over low-power wireless personal area networks (6lowpans): Overview, assumptions, problem statement, and goals. RFC 4919, RFC Editor, August 2007. `http://www.rfc-editor.org/rfc/rfc4919.txt`.

[31] Industrial Automation Process Automation (WIA-PA). http://www.industrialwireless.cn/en/06.asp, Last visited: 11.09.2017.

[32] MSB-A2 data sheet. `ftp://ftp.inf.fu-berlin.de/pub/reports/tr-b-08-15.pdf`. Last visited: 10.03.2019.

[33] Xingfa Shen, Zhi Wang, and Youxian Sun. Wireless sensor networks for industrial applications. *Intelligent Control and Automation, 2004. WCICA 2004. Fifth World Congress on*, 4(60304018):3636–3640, 2004.

[34] Pouria Zand, Supriyo Chatterjea, Kallol Das, and Paul Havinga. Wireless Industrial Monitoring and Control Networks: The Journey So Far and the Road Ahead. *Journal of Sensor and Actuator Networks*, 1(2):123–152, 2012.

[35] Tony O'donovan, James Brown, Felix Büsching, Alberto Cardoso, José Cecílio, Pedro Furtado, Paulo Gil, Anja Jugel, Wolf-Bastian Pöttner, Utz Roedig, et al. The ginseng system for wireless monitoring and control: Design and deployment experiences. *ACM Transactions on Sensor Networks (TOSN)*, 10(1):4, 2013.

[36] Kewei Sha, Weisong Shi, and Orlando Watkins. Using wireless sensor networks for fire rescue applications: Requirements and challenges. In *Electro/information Technology, 2006 IEEE International Conference on*, pages 239–244. IEEE, 2006.

[37] K Ogata. Modern control engineering 5th edition. lugar: Upper saddle river, new jersey 07458. *ed: Prentice Hall*, page 55, 2009.

[38] Vehbi C Gungor, Gerhard P Hancke, and Senior Member. Industrial Wireless Sensor Networks : Challenges , Design Principles , and Technical Approaches. *IEEE Transactions on Industrial Electronics*, 56(10):4258–4265, 2009.

[39] Xiangheng Liu and Andrea Goldsmith. Wireless Medium Access Control in Networked Control Systems. *System*.

[40] A. A. S. Kumar et al. An industrial perspective on wireless sensor networks a survey of requirements, protocols, and challenges. *IEEE Communications Surveys & Tutorials*, 16(3):1391–1412, 2014.

[41] Burak Demirel. *Architectures and performance analysis of wireless control systems*. PhD thesis, KTH Royal Institute of Technology, 2015.

[42] Theodore S Rappaport. Wireless communications–principles and practice, (the book end). *Microwave Journal*, 45(12):128–129, 2002.

[43] J. P. Hespanha, P. Naghshtabrizi, and Y. Xu. A survey of recent results in networked control systems. *Proceedings of the IEEE*, 2007.

[44] Zelalem Teffera Abebe. Process control over wireless sensor networks. Master's thesis, 2013.

[45] Girish N Nair, Fabio Fagnani, Sandro Zampieri, and Robin J Evans. Feedback control under data rate constraints: An overview. *Proceedings of the IEEE*, 95(1):108–137, 2007.

[46] U. Raza, P. Kulkarni, and M. Sooriyabandara. Low power wide area networks: An overview. *IEEE Communications Surveys Tutorials*, 19(2):855–873, Secondquarter 2017.

[47] Jia Zhu, Yulong Zou, and Baoyu Zheng. Physical-layer security and reliability challenges for industrial wireless sensor networks. *IEEE Access*, 5:5313–5320, 2017.

[48] Ian F. Akyildiz, Weilian Su, Yogesh Sankarasubramaniam, and Erdal Cayirci. A survey on sensor networks. *IEEE Communications Magazine*, 40(8):102–105, 2002.

[49] Milica Pejanović Đurišić, Zhilbert Tafa, Goran Dimić, and Veljko Milutinović. A survey of military applications of wireless sensor networks. In *Embedded Computing (MECO), 2012 Mediterranean Conference on*, pages 196–199. IEEE, 2012.

[50] Xue Wang, Sheng Wang, and Daowei Bi. Distributed visual-target-surveillance system in wireless sensor networks. *IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics)*, 39(5):1134–1146, 2009.

[51] Hemant Ghayvat et al. Wsn-and iot-based smart homes and their extension to smart buildings. *Sensors*, 15(5):10350–10379, 2015.

[52] K. Kientopf, S. Raza, S. Lansing, and M. Güneş. Service management platform to support service migrations for iot smart city applications. In *2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, pages 1–5, Oct 2017.

[53] Srijani Mukherjee, Koustabh Dolui, and Soumya Kanti Datta. Patient health management system using e-health monitoring architecture. In *Advance Computing Conference (IACC), 2014 IEEE International*, pages 400–405. IEEE, 2014.

[54] Ronghua Xu, Hongjun Dai, Zhiping Jia, Meikang Qiu, and Bin Wang. A piecewise geometry method for optimizing the motion planning of data mule in tele-health wireless sensor networks. *Wireless networks*, 20(7):1839–1858, 2014.

[55] George Dimitrakopoulos and Panagiotis Demestichas. Intelligent transportation systems. *IEEE Vehicular Technology Magazine*, 5(1):77–84, 2010.

[56] FJ Pierce and TV Elliott. Regional and on-farm wireless sensor networks for agricultural systems in eastern washington. *Computers and electronics in agriculture*, 61(1):32–43, 2008.

[57] Leon Evers and Paul Havinga. Supply chain management automation using wireless sensor networks. In *Mobile Adhoc and Sensor Systems, 2007. MASS 2007. IEEE International Conference on*, pages 1–3. IEEE, 2007.

[58] Rabiaa ELkamel and Adnane Cherif. Energy-efficient routing protocol to improve energy consumption in wireless sensors networks. *International Journal of Communication Systems*, 30(17), 2017.

[59] Hamidreza Salarian, Kwan-Wu Chin, and Fazel Naghdy. Coordination in wireless sensor–actuator networks: a survey. *Journal of Parallel and Distributed Computing*, 72(7):856–867, 2012.

[60] Wireless Sensor and Actor Networks (WSAN). http://bwn.ece.gatech.edu/actors/index.html, Last visited: 10.12.2017.

[61] Ian F. Akyildiz and Ismail H. Kasimoglu. Wireless sensor and actor networks: Research challenges. *Ad Hoc Networks*, 2(4):351–367, 2004.

[62] Johan Åkerberg, Mikael Gidlund, and Mats Björkman. Future research challenges in wireless sensor and actuator networks targeting industrial automation. In *Proceeding of the International Conference on Industrial Informatics*, pages 410–415. IEEE, 2011.

[63] Andreas Frotzscher, Ulf Wetzker, Matthias Bauer, Markus Rentschler, Matthias Beyer, Stefan Elspass, and Henrik Klessig. Requirements and current solutions of wireless communication in industrial automation. In *Proceeding of the IEEE International Conference on Communications Workshops (ICC)*, pages 67–72. IEEE, 2014.

[64] N. J. Ploplys, P. A. Kawka, and A. G. Alleyne. Closed-loop control over wireless networks. *IEEE Control Systems Magazine*, 24(3):58–71, June 2004.

[65] Federico Civerchia, Stefano Bocchino, Claudio Salvadori, Enrico Rossi, Luca Maggiani, and Matteo Petracca. Industrial internet of things monitoring solution for advanced predictive maintenance applications. *Journal of Industrial Information Integration*, 2017.

[66] C. Ebert and K. Shankar. Industry trends 2017. *IEEE Software*, 34(2):112–116, Mar 2017.

[67] Li Gui. *A transport protocol for real-time applications in wireless networked control systems*. PhD thesis, Queensland University of Technology, 2010.

[68] J. H. Taylor, J. Åkerberg, H. M. S. Ibrahim, and M. Gidlund. Safe and secure wireless networked control systems. In *2012 IEEE International Conference on Control Applications*, pages 871–878, Oct 2012.

[69] B. Li, Y. Ma, T. Westenbroek, C. Wu, H. Gonzalez, and C. Lu. Wireless routing and control: A cyber-physical case study. In *2016 ACM/IEEE 7th International Conference on Cyber-Physical Systems (ICCPS)*, pages 1–10, April 2016.

[70] Pangun Park, Carlo Fischione, Alvise Bonivento, Karl H Johansson, and Alberto Sangiovanni-Vincent. Breath: an adaptive protocol for industrial

control applications using wireless sensor networks. *IEEE Transactions on Mobile Computing*, 10(6):821–838, 2011.

[71] Volkan Gunes, Steffen Peter, Tony Givargis, and Frank Vahid. A survey on concepts, applications, and challenges in cyber-physical systems. *KSII Transactions on Internet & Information Systems*, 8(12), 2014.

[72] Abdelmalik Bachir et al. MAC Essentials for Wireless Sensor Networks MAC Essentials for Wireless Sensor Networks. *Communications Surveys & Tutorials*, 12(2):222–248, 2010.

[73] Hua Zhu, Ming Li, Imrich Chlamtac, and Balakrishnan Prabhakaran. A survey of quality of service in ieee 802.11 networks. *IEEE Wireless Communications*, 11(4):6–14, 2004.

[74] Rasool Sadeghi, João Paulo Barraca, and Rui L Aguiar. A survey on cooperative mac protocols in ieee 802.11 wireless networks. *Wireless Personal Communications*, 95(2):1469–1493, 2017.

[75] Yi Zhi Zhao, Chunyan Miao, Maode Ma, Jing Bing Zhang, and Cyril Leung. A survey and projection on medium access control protocols for wireless sensor networks. *ACM Comput. Surv.*, 45(1):7:1—-7:37, 2012.

[76] Petcharat Suriyachai et al. Time-critical data delivery in wireless sensor networks. In *International Conference on Distributed Computing in Sensor Systems*, pages 216–229. Springer, 2010.

[77] Holger Karl and Andreas Willig. *Protocols and architectures for wireless sensor networks*. John Wiley & Sons, 2007.

[78] Ian F Akyildiz and Mehmet Can Vuran. *Wireless sensor networks*, volume 4. John Wiley & Sons, 2010.

[79] Alaa Muqattash and Marwan Krunz. Cdma-based mac protocol for wireless ad hoc networks. In *Proceedings of the 4th ACM international symposium on Mobile ad hoc networking & computing*, pages 153–164. ACM, 2003.

[80] Dario Pompili, Tommaso Melodia, and Ian F Akyildiz. A distributed cdma medium access control for underwater acoustic sensor networks. In *Proc. of Mediterranean Ad Hoc Networking Workshop (Med-Hoc-Net)*, pages 63–70, 2007.

[81] Hwee-Xian Tan and Winston KG Seah. Distributed cdma-based mac protocol for underwater sensor networks. In *Local Computer Networks, 2007. LCN 2007. 32nd IEEE Conference on*, pages 26–36. IEEE, 2007.

[82] Mastooreh Salajegheh, Hamed Soroush, and Antonis Kalis. Hymac: Hybrid tdma/fdma medium access control protocol for wireless sensor networks. In *Personal, Indoor and Mobile Radio Communications, 2007. PIMRC 2007. IEEE 18th International Symposium on*, pages 1–5. IEEE, 2007.

[83] Mohammad Hayajneh, Issa Khalil, and Yasser Gadallah. An ofdma-based mac protocol for under water acoustic wireless sensor networks. In *Proceedings of the 2009 International Conference on Wireless Communications and Mobile Computing: Connecting the World Wirelessly*, pages 810–814. ACM, 2009.

[84] Feng Xia and Azizur Rahim. *MAC Protocols for Cyber-Physical Systems*. Springer, 2015.

[85] N. Abramson. Development of the ALOHANET. *IEEE Transactions on Information Theory*, 31(2):119–123, 1985.

[86] Messaoud Doudou, Djamel Djenouri, Nadjib Badache, and Abdelmadjid Bouabdallah. Synchronous contention-based mac protocols for delay-sensitive wireless sensor networks: A review and taxonomy. *Journal of Network and Computer Applications*, 38:172–184, 2014.

[87] I. Rhee, A. Warrier, M. Aia, J. Min, and M. L. Sichitiu. Z-MAC: A hybrid mac for wireless sensor networks. *IEEE/ACM Transactions on Networking*, 16(3):511–524, June 2008.

[88] Lanny Sitanayah, Cormac J Sreenan, and Kenneth N Brown. Er-mac: A hybrid mac protocol for emergency response wireless sensor networks. In *Sensor Technologies and Applications (SENSORCOMM), 2010 Fourth International Conference on*, pages 244–249. IEEE, 2010.

[89] Tsung-Han Hsieh, Kuei-Ying Lin, and Pi-Chung Wang. A hybrid mac protocol for wireless sensor networks. In *Networking, Sensing and Control (ICNSC), 2015 IEEE 12th International Conference on*, pages 93–98. IEEE, 2015.

[90] Khusvinder Gill, Shuang-Hua Yang, Fang Yao, and Xin Lu. A zigbee-based home automation system. *IEEE Transactions on Consumer Electronics*, 55(2), 2009.

[91] Mohammad reza Akhondi, Alex Talevski, Simon Carlsen, and Stig Petersen. Applications of wireless sensor networks in the oil, gas and resources industries. In *Proceeding of the International Conference on Advanced Information Networking and Applications*, pages 941–948. IEEE, 2010.

[92] Luis Sanchez, Luis Muñoz, Jose Antonio Galache, Pablo Sotres, Juan R Santana, Veronica Gutierrez, Rajiv Ramdhany, Alex Gluhak, Srdjan Krco, Evangelos Theodoridis, et al. SmartSantander: IoT experimentation over a smart city testbed. *Computer Networks*, 61:217–238, 2014.

[93] Emil Jovanov, Aleksandar Milenkovic, Chris Otto, and Piet C De Groen. A wireless body area network of intelligent motion sensors for computer assisted physical rehabilitation. *Journal of NeuroEngineering and rehabilitation*, 2(1):6, 2005.

[94] Jianping Song, Song Han, Al Mok, Deji Chen, Mike Lucas, Mark Nixon, and Wally Pratt. Wirelesshart: Applying wireless technology in real-time industrial process control. In *Real-Time and Embedded Technology and Applications Symposium, 2008. RTAS'08. IEEE*, pages 377–386. IEEE, 2008.

[95] LAN/MAN Standards Committee et al. Part 15.4: wireless medium access control (mac) and physical layer (phy) specifications for low-rate wireless personal area networks (lr-wpans). *IEEE Computer Society*, 2003.

[96] Surjya Ray, Ilker Demirkol, and Wendi Heinzelman. Adv-mac: Analysis and optimization of energy efficiency through data advertisements for wireless sensor networks. *Ad Hoc Networks*, 9(5):876–892, 2011.

[97] Eduardo Casilari, Jose M Cano-García, and Gonzalo Campos-Garrido. Modeling of current consumption in 802.15. 4/zigbee sensor motes. *Sensors*, 10(6):5443–5468, 2010.

[98] IEEE standard for local and metropolitan area networks–part 15.4: Low-rate wireless personal area networks (lr-wpans). *IEEE Std 802.15.4-2011 (Revision of IEEE Std 802.15.4-2006)*, pages 1–314, Sept 2011.

[99] Liqun Hou and Neil W. Bergmann. System requirements for industrial wireless sensor networks. *Emerging Technologies and Factory Automation (ETFA), 2010 IEEE Conference on*, pages 1–8, 2010.

[100] Mario Di Francesco, Giuseppe Anastasi, Marco Conti, Sajal K Das, and Vincenzo Neri. Reliability and energy-efficiency in ieee 802.15. 4/zigbee sensor networks: an adaptive and cross-layer approach. *IEEE Journal on selected areas in communications*, 29(8):1508–1524, 2011.

[101] Jelena Mišić, Shairmina Shafi, and Vojislav B Mišić. Performance limitations of the mac layer in 802.15. 4 low rate wpan. *Computer Communications*, 29(13-14):2534–2541, 2006.

[102] Sofie Pollin, Mustafa Ergen, Sinem Coleri Ergen, Bruno Bougard, Liesbet Van der Perre, Ingrid Moerman, Ahmad Bahai, Pravin Varaiya, and Francky Catthoor. Performance analysis of slotted carrier sense ieee 802.15. 4 medium access layer. *IEEE Transactions on wireless communications*, 7(9), 2008.

[103] Giuseppe Anastasi, Marco Conti, and Mario Di Francesco. A comprehensive analysis of the mac unreliability problem in ieee 802.15. 4 wireless sensor networks. *IEEE Transactions on Industrial Informatics*, 7(1):52–65, 2011.

[104] Anis Koubaa, Mário Alves, and Eduardo Tovar. A comprehensive simulation study of slotted csma/ca for ieee 802.15. 4 wireless sensor networks. In *Proceeding of the IEEE International Workshop on Factory Communication Systems*, pages 183–192. IEEE, 2006.

[105] Mounib Khanafer, Mouhcine Guennoun, and Hussein T Mouftah. A survey of beacon-enabled ieee 802.15. 4 mac protocols in wireless sensor networks. *IEEE Communications Surveys & Tutorials*, 16(2):856–876, 2014.

[106] Tomas Lennvall, Stefan Svensson, and Fredrik Hekland. A comparison of WirelessHART and ZigBee for industrial applications. *IEEE International Workshop on Factory Communication Systems - Proceedings, WFCS*, pages 85–88, 2008.

[107] Zigbee PRO. `https://zigbee.org/zigbee-for-developers/zigbee-pro/`, Last visited: 13.08.2019.

[108] David Rodenas-Herraiz et al. Current trends in wireless mesh sensor networks: A review of competing approaches. *Sensors (Switzerland)*, 13(5):5958–5995, 2013.

[109] Gaetano Patti et al. Introducing multi-level communication in the ieee 802.15. 4e protocol: the multichannel-lldn. In *Emerging Technology and Factory Automation (ETFA), 2014 IEEE*, pages 1–8. IEEE, 2014.

[110] Achim Berger, Markus Pichler, Werner Haselmayr, and Andreas Springer. Energy-efficient and reliable wireless sensor networks-an extension to ieee 802.15. 4e. *EURASIP Journal on Wireless Communications and Networking*, 2014(1):126, 2014.

[111] T. Watteyne, M. Palattella, and L. Grieco. Using IEEE 802.15.4e time-slotted channel hopping (TSCH) in the internet of things (iot): Problem statement. Internet Requests for Comments, May 2015. `http://www.rfc-editor.org/rfc/rfc7554.txt`.

[112] KSJ Pister and L Doherty. Technical overview of time synchronized mesh protocol (TSMP). In *International Symposium on Parallel and Distributed Computing and Systems*, 2006.

[113] Delphine Christin, Parag S Mogre, and Matthias Hollick. Survey on wireless sensor network technologies for industrial automation: The security and quality of service perspectives. *Future Internet*, 2(2):96–125, 2010.

[114] Kristofer S. J. Pister and Lance Doherty. TSMP: Time synchronized mesh protocol. *Pdcs*, pages 391–398, 2008.

[115] Mark Nixon and TX Round Rock. A comparison of wirelesshart and isa100. 11a. *Whitepaper, Emerson Process Management*, pages 1–36, 2012.

[116] Delphine Christin et al. Survey on Wireless Sensor Network Technologies for Industrial Automation: The Security and Quality of Service Perspectives. *Future Internet*, 2(2):96–125, 2010.

[117] Márcio S Costa and Jorge LM Amaral. Analysis of wireless industrial automation standards: Isa-100.11 a and wirelesshart. *InTech Magazine*, 2012.

[118] Fadillah Purnama Rezha and Soo Young Shin. Performance evaluation of isa100. 11a industrial wireless network. 2013.

[119] Stig Petersen and Simon Carlsen. WirelessHART versus ISA100.11a: The format war hits the factory floor. *IEEE Industrial Electronics Magazine*, 5(4):23–34, 2011.

[120] Chinese Industrial Wireless Alliance (CIWA). http://www.industrialwireless.cn/en/06.asp, Last visited: 29.09.2017.

[121] International Electrotechnical Commission (IEC). `http://www.iec.ch/`, Last visited: 01.10.2017.

[122] Wei Liang, Xiaoling Zhang, Yang Xiao, Fuqiang Wang, Peng Zeng, and Haibin Yu. Survey and experiments of wia-pa specification of industrial wireless network. *Wireless Communications and Mobile Computing*, 11(8):1197–1212, 2011.

[123] Heng Wang, Xinyu Wei, and Ping Wang. A transmission scheme of ipv6 packets over wia-pa networks. In *Chinese Automation Congress (CAC), 2015*, pages 1137–1142. IEEE, 2015.

[124] Richard Zurawski. *Industrial communication technology handbook*. Industrial Information Technology. CRC Press, 2014.

[125] Leopoldo Angrisani, Matteo Bertocco, Daniele Fortin, and Alessandro Sona. Experimental study of coexistence issues between ieee 802.11 b and ieee 802.15. 4 wireless networks. *IEEE Transactions on Instrumentation and Measurement*, 57(8):1514–1523, 2008.

[126] EEE802.15.2: Coexistence of Wireless Personal Area Networks with Other Wireless Devices Operating in Unlicensed Frequency Bands.

[127] Axel Sikora and Voicu F Groza. Coexistence of IEEE802.15.4 with other Systems in the 2.4 GHz-ISM-Band. In *Proceeding of IEEE Instrumentation and Measurement Technology Conference*, volume 3, pages 1786–1791. IEEE, 2005.

[128] Sofie Pollin, Ian Tan, Bill Hodge, Carl Chun, and Ahmad Bahai. Harmful coexistence between 802.15. 4 and 802.11: A measurement-based study. In *Proceeding of the International Conference on Cognitive Radio Oriented Wireless Networks and Communications (CrownCom)*, pages 1–6. IEEE, 2008.

[129] Co-existence of IEEE 802.15.4 at 2.4 GHz Application Note. http://www.nxp.com/docs/en/application-note/JN-AN-1079.pdf, Last visited: 08.03.2019.

[130] Su Min Kim, Jo Woon Chong, Chang Yong Jung, Tae Ho Jeon, Jun Hyun Park, You Jin Kang, Seong Hoon Jeong, Min Jeong Kim, and Dan Keun Sung. Experiments on interference and coexistence between zigbee and wlan devices operating in the 2.4 ghz ism band. *Proc. NGPC*, pages 15–19, 2005.

[131] Wenqi Guo, William M Healy, and MengChu Zhou. Impacts of 2.4-ghz ism band interference on ieee 802.15. 4 wireless sensor network reliability in buildings. *IEEE Transactions on Instrumentation and Measurement*, 61(9):2533–2544, 2012.

[132] Yoshihiro Kawahara, Xiaoying Bian, Ryo Shigeta, Rushi Vyas, Manos M Tentzeris, and Tohru Asami. Power harvesting from microwave oven electromagnetic leakage. In *Proceedings of the ACM international joint conference on Pervasive and ubiquitous computing*, pages 373–382. ACM, 2013.

[133] Surveys of Microwave Ovens in U.S. Homes. https://eta.lbl.gov/publications/surveys-microwave-ovens-us-homes, Last Visited: 10.10.2018.

[134] Kaushik R Chowdhury and Ian F Akyildiz. Interferer classification, channel selection and transmission adaptation for wireless sensor networks. In *Proceeding of the International Conference on Communications*, pages 1–5. IEEE, 2009.

[135] Thomas W Rondeau, Mark F D'Souza, and Dennis G Sweeney. Residential microwave oven interference on bluetooth data performance. *IEEE Transactions on Consumer Electronics*, 50(3):856–863, 2004.

[136] Wei Shen, Tingting Zhang, Filip Barac, and Mikael Gidlund. Prioritymac: A priority-enhanced mac protocol for critical traffic in industrial wireless sensor and actuator networks. *IEEE Transactions on Industrial Informatics*, 10(1):824–835, 2014.

[137] Petcharat Suriyachai et al. Implementation of a mac protocol for qos support in wireless sensor networks. In *Pervasive Computing and Communications, 2009. PerCom 2009. IEEE International Conference on*, pages 1–6. IEEE, 2009.

[138] Tao Zheng, Mikael Gidlund, and Johan Åkerberg. Wirarb: A new mac protocol for time critical industrial wireless sensor network applications. *IEEE Sensors Journal*, 16(7):2127–2139, 2016.

[139] Pangun Park, Carlo Fischione, Alvise Bonivento, Karl H Johansson, and Alberto Sangiovanni-Vincent. Breath: an adaptive protocol for industrial control applications using wireless sensor networks. *IEEE Transactions on Mobile Computing*, 10(6):821–838, 2011.

[140] Admar Ajith Kumar Somappa, Knut Øvsthus, and Lars Michael Kristensen. Towards a dual-mode adaptive MAC protocol (DMA-MAC) for feedback-based networked control systems. pages 505–510, 2014.

[141] Thomas Watteyne, Ankur Mehta, and Kris Pister. Reliability through frequency diversity: why channel hopping makes sense. In *Proceedings of the 6th ACM symposium on Performance evaluation of wireless ad hoc, sensor, and ubiquitous networks*, pages 116–123. ACM, 2009.

[142] Thomas Watteyne, Joy Weiss, Lance Doherty, and Jonathan Simon. Industrial IEEE802.15.4e networks: Performance and trade-offs. In *Proceeding of the International Conference on Communications (ICC)*, pages 604–609. IEEE, 2015.

[143] Thomas Watteyne, M Palattella, and L Grieco. Using IEEE 802.15.4e Time-Slotted Channel Hopping (TSCH) in the Internet of Things (IoT): Problem Statement. Technical report, IEEE, 2015.

[144] Alberto Cerpa, Jennifer L. Wong, Miodrag Potkonjak, and Deborah Estrin. Temporal properties of low power wireless links: Modeling and implications on multi-hop routing. In *Proceedings of the 6th ACM International Symposium on Mobile Ad Hoc Networking and Computing*, MobiHoc '05, pages 414–425, New York, NY, USA, 2005. ACM.

[145] X. Vilajosana, K. Pister, and T. Watteyne. Minimal 6tisch configuration draft-ietf-6tisch-minimal-19. Internet Requests for Comments, 25, Jan. 2017, work in progress.

[146] S. Duquennoy, A. Elsts, B. A. Nahas, and G. Oikonomo. Tsch and 6tisch for contiki: Challenges, design and evaluation. In *2017 13th International Conference on Distributed Computing in Sensor Systems (DCOSS)*, pages 11–18, June 2017.

[147] D. Dujovne, T. Watteyne, X. Vilajosana, and P. Thubert. 6tisch: deterministic ip-enabled industrial internet (of things). *IEEE Communications Magazine*, 52(12):36–41, December 2014.

[148] Timothy Claeys. *Initialisation of a wireless sensor network with the time.* PhD thesis, Grenoble INP, 2015.

[149] Harrison Kurunathan, Ricardo Severino, Anis Koubaa, and Eduardo Tovar. Towards worst-case bounds analysis of the ieee 802.15. 4e. In *Work in Progress Session, 22nd IEEE Real-Time Embedded Technology & Applications Symposium.* Institute of Electrical and Electronics Engineers, 2016.

[150] M. Vilgelm, M. Gürsu, S. Zoppi, and W. Kellerer. Time slotted channel hopping for smart metering: Measurements and analysis of medium access. In *2016 IEEE International Conference on Smart Grid Communications (SmartGridComm)*, pages 109–115, Nov 2016.

[151] S. Ben Yaala and R. Bouallegue. On mac layer protocols towards internet of things: From ieee802.15.4 to ieee802.15.4e. In *2016 24th International Conference on Software, Telecommunications and Computer Networks (SoftCOM)*, pages 1–5, Sept 2016.

[152] A. Elsts, X. Fafoutis, J. Pope, G. Oikonomou, R. Piechocki, and I. Craddock. Scheduling high-rate unpredictable traffic in ieee 802.15.4 tsch networks. In *2017 13th International Conference on Distributed Computing in Sensor Systems (DCOSS)*, pages 3–10, June 2017.

[153] M. R. Palattella, N. Accettura, L. A. Grieco, G. Boggia, M. Dohler, and T. Engel. On optimal scheduling in duty-cycled industrial iot applications using ieee802.15.4e tsch. *IEEE Sensors Journal*, 13(10):3655–3666, Oct 2013.

[154] Ren-Hung Hwang, Chih-Chiang Wang, and Wu-Bin Wang. A distributed scheduling algorithm for ieee 802.15. 4e wireless sensor networks. *Computer Standards & Interfaces*, 52:63–70, 2017.

[155] Kyeong Tae Kim, Haeyong Kim, Huing Park, and Seon-Tae Kim. An industrial iot mac protocol based on ieee 802.15. 4e tsch for a large-scale network. In *Advanced Communication Technology (ICACT), 2017 19th International Conference on*, pages 721–724. IEEE, 2017.

[156] Domenico De Guglielmo, Simone Brienza, and Giuseppe Anastasi. A model-based beacon scheduling algorithm for ieee 802.15. 4e tsch networks. In

World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2016 IEEE 17th International Symposium on A, pages 1–9. IEEE, 2016.

[157] Tim van der Lee, Saleem Raza, George Exarchakos, and Mesut Günes. Towards co-located TSCH networks: An inter-network interference perspective. In *2018 IEEE Global Communications Conference: Ad Hoc and Sensor Networks (Globecom2018 AHSN)*, Abu Dhabi, United Arab Emirates, December 2018.

[158] S. Ben Yaala, F. Theoleyre, and R. Bouallegue. Performance study of co-located IEEE 802.15.4-TSCH networks: Interference and coexistence. In *2016 IEEE Symposium on Computers and Communication (ISCC)*, pages 513–518, June 2016.

[159] Zach Shelby and Carsten Bormann. *6LoWPAN: The wireless embedded Internet*, volume 43. John Wiley & Sons, 2011.

[160] Jonathan W Hui and David E Culler. Extending ip to low-power, wireless personal area networks. *IEEE Internet Computing*, 12(4), 2008.

[161] P Thubert, T Watteyne, R Struik, and M Richardson. An architecture for ipv6 over the tsch mode of ieee 802.15. 4. draft-ietf-6tisch-architecture-10. *IETF Draft, March*, 2015.

[162] P Thubert, A Brandt, J Hui, R Kelsey, P Levis, K Pister, R Struik, JP Vasseur, and R Alexander. RPL: IPv6 routing protocol for low power and lossy networks. *RFC 6550*, 2012.

[163] Z Shelby, K Hartke, and C Bormann. Rfc 7252-the constrained application protocol (coap). *Internet Engineering T ask Force (IETF)*, 2014.

[164] Q Wang, X Vilajosana, and T Watteyne. 6tisch operation sublayer (6top) draft-wang-6tisch-6top-sublayer-01. Technical report, Internet-Draft. IETF, 2014.

[165] H. Kim, J. Ko, D. E. Culler, and J. Paek. Challenging the ipv6 routing protocol for low-power and lossy networks (rpl): A survey. *IEEE Communications Surveys Tutorials*, 19(4):2502–2525, Fourthquarter 2017.

[166] P Levis, Thomas H. Clausen, Omprakash Gnawali, Jonathan Hui, and JeongGil Ko. The Trickle Algorithm. RFC 6206, March 2011.

[167] Isam Ishaq, David Carels, Girum Teklemariam, Jeroen Hoebeke, Floris Abeele, Eli Poorter, Ingrid Moerman, and Piet Demeester. Ietf standardization in the field of the internet of things (iot): a survey. *Journal of Sensor and Actuator Networks*, 2(2):235–287, 2013.

[168] K. Kritsis, G. Z. Papadopoulos, A. Gallais, P. Chatzimisios, and F. Théoleyre. A tutorial on performance evaluation and validation methodology for low-power and lossy networks. *IEEE Communications Surveys Tutorials*, 20(3):1799–1825, thirdquarter 2018.

[169] G. Gaillard, D. Barthel, F. Theoleyre, and F. Valois. Service level agreements for wireless sensor networks: A wsn operator's point of view. In *2014 IEEE Network Operations and Management Symposium (NOMS)*, pages 1–8, May 2014.

[170] Stênio Fernandes. *Performance Evaluation for Network Services, Systems and Protocols*. Springer, 2017.

[171] Klaus Wehrle, Mesut Günes, and James Gross. *Modeling and tools for network simulation*. Springer Science & Business Media, 2010.

[172] Xuefeng Yin and Xiang Cheng. *Propagation channel characterization, parameter estimation, and modeling for wireless communications*. John Wiley & Sons, 2016.

[173] OMNeT++ Discrete Event Simulator. `https://omnetpp.org/doc/omnetpp/manual/`. Version 5.2, Last visited: 30.03.2018.

[174] Antonio Virdis and Michael Kirsche. Recent advances in network simulation.

[175] Andreas Köpke, Michael Swigulski, Karl Wessel, Daniel Willkomm, PT Haneveld, Tom EV Parker, Otto W Visser, Hermann S Lichte, and Stefan Valentin. Simulating wireless and mobile networks in omnet++ the mixim vision. In *Proceedings of the 1st international conference on Simulation tools and techniques for communications, networks and systems & workshops*, page 71. ICST (Institute for Computer Sciences, Social-Informatics and ..., 2008.

[176] omnetpp-models/mixim. `https://github.com/omnetpp-models/mixim`. Last visited: 05.06.2018.

[177] INETMANET Framework. https://github.com/aarizaq/inetmanet-3.x. Last visited: 20.02.2018.

[178] Contiki: The open source os for the internet of things. http://www.contiki-os.org/. Last visited: 20.04.2018.

[179] Contiki-NG: The OS for Next Generation IoT Devices. https://www.contiki-ng.org/. Last visited: 20.04.2019.

[180] Matplotlib tutorial – a complete guide to python plot w/ examples. https://www.machinelearningplus.com/plots/matplotlib-tutorial-complete-guide-python-plot-examples/. Last visited: 18.06.2019.

[181] I. Juc, O. Alphand, R. Guizzetti, M. Favre, and A. Duda. Energy consumption and performance of IEEE 802.15.4e TSCH and DSME. In *IEEE Wireless Communications and Networking Conference*, pages 1–7, April 2016.

[182] L. Angrisani, M. Bertocco, D. Fortin, and A. Sona. Experimental study of coexistence issues between IEEE 802.11b and IEEE 802.15.4 wireless networks. *IEEE Transactions on Instrumentation and Measurement*, 57(8):1514–1523, Aug 2008.

[183] L. M. Feeney, M. Frey, V. Fodor, and M. Gunes. Modes of inter-network interaction in beacon-enabled IEEE 802.15.4 networks. In *14th Annual Mediterranean Ad Hoc Networking Workshop (MED-HOC-NET)*, pages 1–8, June 2015.

[184] N. Nordin et al. Effects and implications of beacon collisions in co-located IEEE 802.15.4 networks. In *2012 IEEE Vehicular Technology Conference (VTC Fall)*, pages 1–5, Sept 2012.

[185] D. Stanislowski, X. Vilajosana, Q. Wang, T. Watteyne, and K. S. J. Pister. Adaptive synchronization in IEEE 802.15.4e networks. *IEEE Transactions on Industrial Informatics*, 10(1):795–802, Feb 2014.

[186] Y. Al-Nidawi, H. Yahya, and A. H. Kemp. Impact of mobility on the iot mac infrastructure: IEEE 802.15.4e TSCH and LLDN platform. In *2015 IEEE 2nd World Forum on Internet of Things (WF-IoT)*, pages 478–483, Dec 2015.

[187] Y. Al-Nidawi and A. H. Kemp. Mobility aware framework for time-slotted channel hopping IEEE 802.15.4e sensor networks. *IEEE Sensors Journal*, 15(12):7112–7125, Dec 2015.

[188] Simon Duquennoy, Beshr Al Nahas, Olaf Landsiedel, and Thomas Watteyne. Orchestra: Robust mesh networks through autonomously scheduled tsch. In *Proceedings of the 13th ACM Conference on Embedded Networked Sensor Systems*, SenSys '15, pages 337–350, New York, NY, USA, 2015. ACM.

[189] Tracy Camp, Jeff Boleng, and Vanessa Davies. A survey of mobility models for ad hoc network research. *Wireless communications and mobile computing*, 2(5):483–502, 2002.

[190] Long Bao Le, Eytan Modiano, Changhee Joo, and Ness B Shroff. Longest-queue-first scheduling under sinr interference model. In *Proceedings of the eleventh ACM international symposium on Mobile ad hoc networking and computing*, pages 41–50, 2010.

[191] Aravind Iyer, Catherine Rosenberg, and Aditya Karnik. What is the right model for wireless channel interference? *IEEE Transactions on Wireless Communications*, 8(5):2662–2671, 2009.

[192] Texas Instruments. CC2420: 2.4GHz IEEE 802.15.4/ZigBee-ready RF Transceiver. `http://www.ti.com/lit/ds/symlink/cc2420.pdf`, 2007.

Ehrenerklärung

Ich versichere hiermit, dass ich die vorliegende Arbeit ohne unzulässige Hilfe Dritter und ohne Benutzung anderer als der angegebenen Hilfsmittel angefertigt habe; verwendete fremde und eigene Quellen sind als solche kenntlich gemacht. Insbeson- dere habe ich nicht die Hilfe eines kommerziellen Promotionsberaters in Anspruch genommen. Dritte haben von mir weder unmittelbar noch mittelbar geldwerte Leistungen für Arbeiten erhalten, die im Zusammenhang mit dem Inhalt der vorgelegten Dissertation stehen.
Ich habe insbesondere nicht wissentlich:

- Ergebnisse erfunden oder widersprüchliche Ergebnisse verschwiegen,
- statistische Verfahren absichtlich missbraucht, um Daten in ungerechtfertigter Weise zu interpretieren,
- fremde Ergebnisse oder Veröffentlichungen plagiiert,
- fremde Forschungsergebnisse verzerrt wiedergegeben.

Mir ist bekannt, dass Verstöße gegen das Urheberrecht Unterlassungs- und Schadenser- satzansprüche des Urhebers sowie eine strafrechtliche Ahndung durch die Strafver- folgungsbehörden begründen kann. Die Arbeit wurde bisher weder im Inland noch im Ausland in gleicher oder ähnlicher Form als Dissertation eingereicht und ist als Ganzes auch noch nicht veröffentlicht.

Magdeburg, den 15th November, 2019

Saleem Raza

____