Chapman & Hall/CRC
Computer & Information Science Series

From Internet of Things to Smart Cities

Enabling Technologies

Edited by

Hongjian Sun
Chao Wang
Bashar I. Ahmad

CPD CERTIFIED
The CPD Certification Service

CRC Press
Taylor & Francis Group
A CHAPMAN & HALL BOOK

From Internet of Things to Smart Cities

Enabling Technologies

CHAPMAN & HALL/CRC
COMPUTER and INFORMATION SCIENCE SERIES

Series Editor: Sartaj Sahni

PUBLISHED TITLES

ADVERSARIAL REASONING: COMPUTATIONAL APPROACHES TO READING THE OPPONENT'S MIND
Alexander Kott and William M. McEneaney

COMPUTER-AIDED GRAPHING AND SIMULATION TOOLS FOR AUTOCAD USERS
P. A. Simionescu

DELAUNAY MESH GENERATION
Siu-Wing Cheng, Tamal Krishna Dey, and Jonathan Richard Shewchuk

DISTRIBUTED SENSOR NETWORKS, SECOND EDITION
S. Sitharama Iyengar and Richard R. Brooks

DISTRIBUTED SYSTEMS: AN ALGORITHMIC APPROACH, SECOND EDITION
Sukumar Ghosh

ENERGY-AWARE MEMORY MANAGEMENT FOR EMBEDDED MULTIMEDIA SYSTEMS: A COMPUTER-AIDED DESIGN APPROACH
Florin Balasa and Dhiraj K. Pradhan

ENERGY EFFICIENT HARDWARE-SOFTWARE CO-SYNTHESIS USING RECONFIGURABLE HARDWARE
Jingzhao Ou and Viktor K. Prasanna

FROM ACTION SYSTEMS TO DISTRIBUTED SYSTEMS: THE REFINEMENT APPROACH
Luigia Petre and Emil Sekerinski

FROM INTERNET OF THINGS TO SMART CITIES: ENABLING TECHNOLOGIES
Hongjian Sun, Chao Wang, and Bashar I. Ahmad

FUNDAMENTALS OF NATURAL COMPUTING: BASIC CONCEPTS, ALGORITHMS, AND APPLICATIONS
Leandro Nunes de Castro

HANDBOOK OF ALGORITHMS FOR WIRELESS NETWORKING AND MOBILE COMPUTING
Azzedine Boukerche

HANDBOOK OF APPROXIMATION ALGORITHMS AND METAHEURISTICS
Teofilo F. Gonzalez

HANDBOOK OF BIOINSPIRED ALGORITHMS AND APPLICATIONS
Stephan Olariu and Albert Y. Zomaya

HANDBOOK OF COMPUTATIONAL MOLECULAR BIOLOGY
Srinivas Aluru

HANDBOOK OF DATA STRUCTURES AND APPLICATIONS
Dinesh P. Mehta and Sartaj Sahni

PUBLISHED TITLES CONTINUED

HANDBOOK OF DYNAMIC SYSTEM MODELING
Paul A. Fishwick

HANDBOOK OF ENERGY-AWARE AND GREEN COMPUTING
Ishfaq Ahmad and Sanjay Ranka

HANDBOOK OF GRAPH THEORY, COMBINATORIAL OPTIMIZATION, AND ALGORITHMS
Krishnaiyan "KT" Thulasiraman, Subramanian Arumugam, Andreas Brandstädt, and Takao Nishizeki

HANDBOOK OF PARALLEL COMPUTING: MODELS, ALGORITHMS AND APPLICATIONS
Sanguthevar Rajasekaran and John Reif

HANDBOOK OF REAL-TIME AND EMBEDDED SYSTEMS
Insup Lee, Joseph Y-T. Leung, and Sang H. Son

HANDBOOK OF SCHEDULING: ALGORITHMS, MODELS, AND PERFORMANCE ANALYSIS
Joseph Y.-T. Leung

HIGH PERFORMANCE COMPUTING IN REMOTE SENSING
Antonio J. Plaza and Chein-I Chang

HUMAN ACTIVITY RECOGNITION: USING WEARABLE SENSORS AND SMARTPHONES
Miguel A. Labrador and Oscar D. Lara Yejas

IMPROVING THE PERFORMANCE OF WIRELESS LANs: A PRACTICAL GUIDE
Nurul Sarkar

INTEGRATION OF SERVICES INTO WORKFLOW APPLICATIONS
Paweł Czarnul

INTRODUCTION TO NETWORK SECURITY
Douglas Jacobson

LOCATION-BASED INFORMATION SYSTEMS: DEVELOPING REAL-TIME TRACKING APPLICATIONS
Miguel A. Labrador, Alfredo J. Pérez, and Pedro M. Wightman

METHODS IN ALGORITHMIC ANALYSIS
Vladimir A. Dobrushkin

MULTICORE COMPUTING: ALGORITHMS, ARCHITECTURES, AND APPLICATIONS
Sanguthevar Rajasekaran, Lance Fiondella, Mohamed Ahmed, and Reda A. Ammar

PERFORMANCE ANALYSIS OF QUEUING AND COMPUTER NETWORKS
G. R. Dattatreya

THE PRACTICAL HANDBOOK OF INTERNET COMPUTING
Munindar P. Singh

SCALABLE AND SECURE INTERNET SERVICES AND ARCHITECTURE
Cheng-Zhong Xu

PUBLISHED TITLES CONTINUED

SOFTWARE APPLICATION DEVELOPMENT: A VISUAL C++®, MFC, AND STL TUTORIAL
Bud Fox, Zhang Wenzu, and Tan May Ling

SPECULATIVE EXECUTION IN HIGH PERFORMANCE COMPUTER ARCHITECTURES
David Kaeli and Pen-Chung Yew

TRUSTWORTHY CYBER-PHYSICAL SYSTEMS ENGINEERING
Alexander Romanovsky and Fuyuki Ishikawa

VEHICULAR NETWORKS: FROM THEORY TO PRACTICE
Stephan Olariu and Michele C. Weigle

X-Machines for Agent-Based Modeling: FLAME Perspectives
Mariam Kiran

From Internet of Things to Smart Cities

Enabling Technologies

Edited by

Hongjian Sun

Durham University, UK

Chao Wang

Tongji University, Shanghai, China

Bashar I. Ahmad

University of Cambridge, UK

CRC Press
Taylor & Francis Group
Boca Raton London New York

CRC Press is an imprint of the
Taylor & Francis Group, an **informa** business

A CHAPMAN & HALL BOOK

CRC Press
Taylor & Francis Group
6000 Broken Sound Parkway NW, Suite 300
Boca Raton, FL 33487-2742

Printed on acid-free paper
Version Date: 20170720

International Standard Book Number-13: 978-1-4987-7378-2 (Hardback)

Visit the Taylor & Francis Web site at
http://www.taylorandfrancis.com

and the CRC Press Web site at
http://www.crcpress.com

This book is dedicated to my parents Mr Shan Sun and Ms Lijun Chen, with love (actually they cannot read English).

This book is dedicated to my wife Jing, and my children Jessica Sun and William Sun, with love, too (actually my children cannot read books yet, just sometimes pretend to be reading stories).

But let's see how fast they can learn English and when they are able to understand the technologies in this book.

Hongjian Sun
Durham, United Kingdom
27 October 2016

This book is dedicated to my family and especially my baby daughter, Xiaoyun.

I would also like to acknowledge the support of the National Natural Science Foundation of China (Grants 61401314 and 61331009), and the EU FP7 QUICK project (PIRSES-GA-2013-612652).

Chao Wang

Contents

Preface

Nowadays we are facing numerous environmental, technological, societal and economic challenges, including climate change, limited energy resources, aging populations and economic restructuring. To address these challenges, it becomes of vital importance to deploy information and communication technologies (ICT) throughout our homes and cities for enabling real-time responses to these challenges, for example, to reduce carbon emission, to improve resource utilization efficiency and to promote active engagement of citizens. However, such an ambitious target will require sustained efforts from the Societies of Communications, Signal Processing and Computing, etc., over the years to come.

This book aims to facilitate this sustained effort for introducing the latest ICT enabling technologies and for promoting international collaborations across Societies and sectors, and eventually demonstrating them to the general public. As such, this book consists of three tightly coupled parts:

- Part I: From Machine-to-Machine Communications to Internet of Things. We will introduce the evolvement of enabling technologies from basic machine-to-machine communications to Internet of Things technologies;

- Part II: Data Era: Data Analytic and Security. We will focus on the state-of-the-art data analytic and security techniques;

- Part III: Towards Smart World from Interfaces to Homes to Cities. We will discuss the design of human-machine interface that facilitates the integration of humans to smart homes and cities, either as decision–makers or as knowledge feeders to networks.

DISCLAIMER

We sincerely thank all contributors, who are world-leading experts in their research fields, for contributing chapters to this book. Due to the time limit, there might be errors or typos in this book, but as editors we tried our best to correct them. If you found any errors or typos, please feel free to contact one of our editors.

Editors:
Hongjian Sun, Email: hongjian.sun@durham.ac.uk;
Chao Wang, Email: chaowang@tongji.edu.cn;
Bashar Ahmad, Email: bia23@cam.ac.uk.

I

From Machine-to-Machine Communications to Internet of Things

CHAPTER 1

From Machine-to-Machine Communications to Internet of Things: Enabling Communication Technologies

Hamidreza Shariatmadari

Aalto University

Sassan Iraji

Aalto University, Klick Technologies Ltd.

Riku Jäntti

Aalto University

CONTENTS

1.1 INTRODUCTION

The term Internet of Things (IoT) was first coined by Kevin Ashton in the late 90s, but in reality, IoT goes back a lot further than that. At the beginning it was only a vision but today with the development of communication technologies, and in particular wireless communications, it is becoming rapidly a reality in different domains and sectors [1]. IoT and its enabling services are revolutionizing the way we live and creating huge growth in our economy. According to IoT paradigm, everything and everyone can be part of the Internet. This vision redefines the way people interact with each other and objects they are surrounded by. With the development of communication technologies, billions of IoT devices are currently connected and it is expected there will be a few tens of billions connected devices within the next five years [2]. At the core of IoT, machine-to-machine (M2M) communications or machine-type communications (MTC) plays the fundamental role by providing connectivity between devices and servers. In that regard, it is concluded that IoT is a broader term, which contains devices, M2M communications, and data processing [3]. Thus, IoT vision cannot be materialized without providing efficient M2M communications.

IoT is constantly evolving by envisioning new services and applications in various domains. The envisioned services are associated with a diverse range of communication requirements. This fact has resulted in the emergence of different wireless communication solutions; generally, each solution satisfies a set of requirements. Although the plethora of communication solutions gives the opportunity to choose a proper solution according to the target application, it hinders the wide and fast deployment of the application. In order to overcome such limitations, extensive efforts are being undertaken to enhance the current solutions for supporting a wider range of applications. Meanwhile, the cellular standardization forums are also trying to consider the IoT vision in the development of the next generation of cellular systems.

The goal of this chapter is to make the readers familiar with the most important connectivity solutions for enabling M2M communications and supporting IoT applications. The remainder of the chapter is organized as follows. Section 1.2 discusses some of the IoT services and applications, along with their requirements. Section 1.3 describes some of the existing M2M connectivity technologies and their potentials for supporting IoT applications. Section 1.4 presents the future directions that enable a better support of M2M communications in the cellular systems. Finally, the chapter is concluded in Section 1.5.

1.2 IoT APPLICATIONS AND THEIR REQUIREMENTS

IoT has a wide range of applications in various sectors and domains [4], [5]. The applications can improve the ways people live, provide better interactions with the environment and facilitate the growth in the economy. Some of the viable IoT applications can be categorized as follows.

- **Transportation:** There are applications for transportation systems that help in monitoring the traffic, improving the road safety, and facilitating the assisted driving. Indeed, public safety is becoming an important concern for the increasing number of vehicles on the roads.

- **Monitoring:** Monitoring applications provide the real-time environmental observations enabled by deployed sensors.

- **Wearables:** The wearable devices can be utilized in game and leisure industries, also for the purposes of fitness, wellness, and health monitoring, which are increasingly emerging domains.

- **Smart environment:** The considered applications improve the efficiency of the environmental utilization from different perspectives, such as energy, resources, and carbon footprint. Some of the applications are applicable for smart homes, building automation, and smart cities.

- **Security:** The security applications are applicable to private residential, commercial, and public locations. They can offer remote surveillance, remote alarm, personal tracking, and public infrastructure protection.

- **Utilities:** There are applications that enable remote monitoring and controlling of user consumptions, such as water, gas, and electricity utilities. Other important applications are related to smart grids, which can efficiently balance between the production and consumption of electricity in large systems.

- **Industrial Internet:** Connecting industrial plants to the Internet facilitates the process management and improves the production. These can be achieved by support of logistics, business analytics, predictive maintenance, and factory automation.

The IoT applications, including those mentioned above, have different characteristics. The application characteristics imply constraints on the devices and underlying communications, and also determine how the data should be gathered and processed [3], [6], [7]. Some concerns related to the end devices are power consumption, computational abilities, size, and cost. The parameters that entail constraints on the communications include: the minimum transmission rate, transmission reliability, the maximum tolerable latency, security, mobility, and the number of supported devices. With increasing the number of IoT devices, the procedures of data gathering and processing are becoming more complex. Relevant concerns are related to the level of data processing locally, message routing, and information extraction. The system design for IoT applications requires the joint considerations of different elements, i.e., device, communication technology, and data processing. For instance, the low power consumption for the end device cannot be achieved unless the device consumes very low energy for sensing, processing, and transmitting data.

The M2M communications, as the underlying infrastructure for IoT connectivity, faces different data traffic types and deployment scenarios compared to other human-centric communications. General applications that directly interact with human users require transmitting high amounts of data only during the active periods. In addition, a limited number of users are in active mode at a time. On the contrary, many IoT applications are involved with short amounts of data, periodically generated by a massive number of devices. Some other applications, such as mission-critical applications, require reliable data transmissions with very low-latency. Excessive coverage is essential for those devices that are deployed in remote areas or in places with limited accessibility.

The diverse range of application requirements has hindered the development of a single solution for providing M2M communications. Thus, various wireless technologies have emerged, each one addressing a set of requirements, to support IoT applications. The next section describes some of the existing connectivity solutions, their features, and the supported applications.

1.3 IoT CONNECTIVITY LANDSCAPE

IoT systems are generally comprised of devices, or objects that need to exchange data with each other, or with a central server. As shown in Figure 1.1, the interconnection of the devices and the server can be provided by a local-based network or a cloud-based network. In the local-based network, the server runs the applications and interacts with the devices through the access points (APs). The server can provide Internet access for the devices in the network to make them remotely accessible.

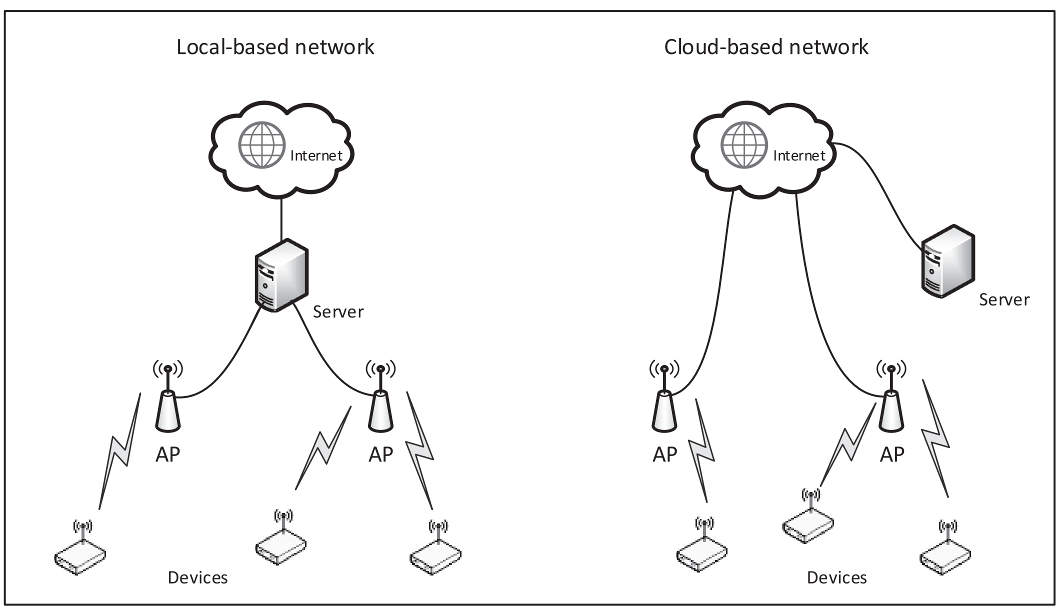

Figure 1.1 Typical network topologies for IoT.

The advantage of this topology is the high level of reliability as the applications can run even if the Internet access fails. In the cloud-based network, the devices and the server perform data exchange through the Internet, entailing all data flow is directed to the Internet. Hence, the stable Internet connection is essential for running the applications. This topology facilitates the scalability of application deployment as the devices can be deployed anywhere as long as they have the Internet access. In addition, the application can be run in a cloud server which eliminates the need of a dedicated server.

Wireless technologies are preferred to provide connectivity for IoT devices due to the ease of deployment, elimination of wiring cost, and mobility support. Initially, many manufacturers developed IoT applications using their own proprietary wireless systems. This approach has brought different technical issues, such as complexity of system design, and lack of compatibility. For instance, products from different manufacturers could not be easily integrated in a system. Those limitations could not be eliminated without employing standardized wireless technologies. In part, some standardization forums put effort to modify the existing wireless systems to support IoT applications. In addition, several wireless solutions have emerged, optimized for IoT applications. The rest of this section describes some of these technologies.

1.3.1 IEEE 802.15.4

IEEE 802.15.4 defines the physical (PHY) layer and medium access control (MAC) layer specifications for low-rate wireless personal area networks (LR-WPANs) [8]. It is designed to provide local connectivity for devices with low power consumption and over relatively short distances. The IEEE 802.15 working group released the first edition of the standard in 2003 and maintained it by providing additional amendments. The standard is based on the open system interconnection (OSI) model, without specifying the higher layers. The specifications of PHY and MAC layers enable interoperability between devices developed by different manufacturers. The upper layers can be designed and optimized according to the specific application. Indeed, various network protocols have been designed on top of IEEE 802.15.4 to support a wide range of applications, such as IPv6 over low power wireless personal area networks (6LoWPAN), ZigBee, WirelessHART, and ISA100.11a [9], [10], [11].

IEEE 802.15.4-2003 specifies the PHY layer over three different unlicensed industrial, scientific, and medical (ISM) frequency bands. The offered data rates depend on the operating frequency band, corresponding to 20 kbps in 868 MHz, 40 kbps in 915 MHz, and 250 kbps in 2.4 GHz. The higher data rates are offered in the later revisions of the standard. In most of the countries, the 2.4 GHz radio is utilized dominantly due to the higher data rate and the availability of the frequency band. In this frequency band, the total of 16 channels is available for network operation, each with 2 MHz bandwidth. The IEEE 802.15.4 transmits data with low power, i.e., less than 1 dBm. The low transmission power limits the communication range, typically less than 100 m, and also makes the data transmission susceptible to radio interference from other competing technologies operating in this frequency band, such as WiFi and Bluetooth [12].

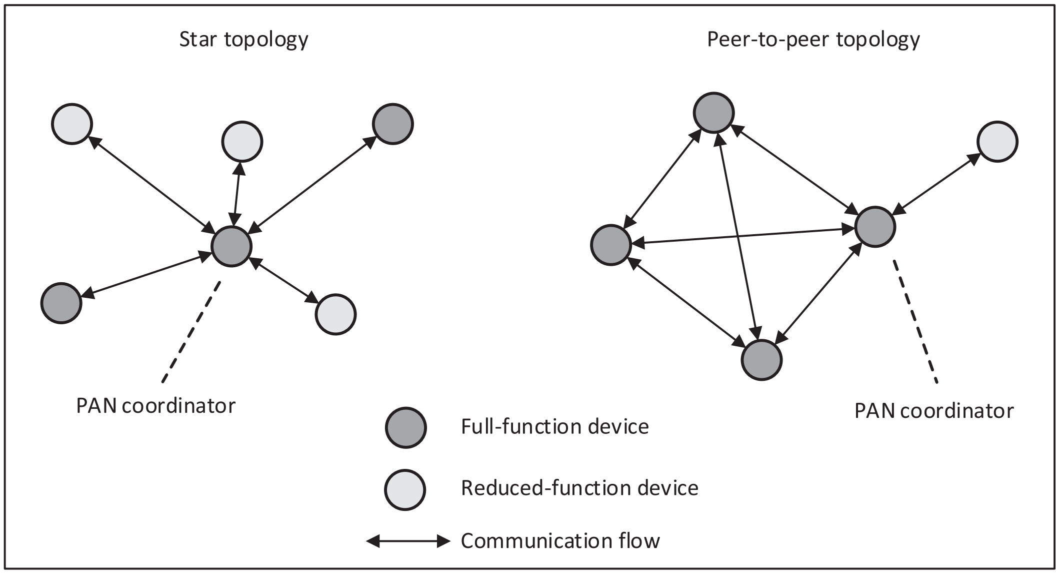

Figure 1.2 Network topologies in IEEE 802.15.4.

The MAC layer in IEEE 802.15.4 handles the access to the radio channel and provides an interface between the service specific convergence sublayer (SSCS) and PHY layer. It is also responsible for network synchronization, supporting device security, and providing a reliable link between two peer MAC entities. Two different device types are defined for the IEEE 802.15.4 network: a full-function device (FFD) that supports all network functionalities, and reduced function device (RFD) with reduced network functionalities [8], [13]. The network can utilize star or peer-to-peer topologies, as illustrated in Figure 1.2. In the star topology, devices can only exchange information with a single central controller unit in the network, known as the personal area network (PAN) coordinator. The PAN coordinator is responsible for managing the entire network. In the peer-to-peer topology, FFD devices have additional ability to communicate directly with each other.

The IEEE 802.15.4-2003 standard is complemented with amendments to further enhance the performance and offer additional functionalities that are required for some specific IoT applications. Some of these amendments are as follows.

- **IEEE 802.15.4a:** This amendment specifies two additional PHY layers, using ultra-wide band (UWB) and chirp spread spectrum (CSS) [13]. The UWB PHY enables precision ranging that can be utilized for positioning purpose. The CSS PHY provides robust data transmission over a large distance for devices moving at high speed, applicable for vehicular communications.

- **IEEE 802.15.4b:** This amendment offers the higher data rates, 200 kbps in 868 MHz and 500 kbps in 915 MHz bands.

- **IEEE 802.15.4e:** This amendment features functional improvements for the MAC layer to support industrial applications more efficiently [14]. It includes three new MAC schemes: time slotted channel hopping (TSCH), deterministic and synchronous multi-channel extension (DSME), and low latency deterministic network (LLDN). The new MAC options facilitate more reliable communications with low-latency.

- **IEEE 802.15.4q:** This amendment specifies two alternate PHY layers, based on amplitude shift keying with ternary amplitude sequence spreading (TASK) and rate switch-Gaussian frequency shift keying (RS-GFSK), to achieve ultra-low power consumption.

- **IEEE 802.15.4r:** This amendment provides PHY and MAC extensions to enable radio-based distance measurements.

- **IEEE 802.15.4s:** This amendment defines MAC functionalities that enable spectrum resource management.

- **IEEE 802.15.4t:** This amendment provides a higher data rate of 2 Mbps in 2.4 GHz band.

IEEE 802.15.4 enables a flexible integration of network stacks and protocols for supporting different applications. 6LoWPAN is a network protocol from the Internet Engineering Task Force (IETF) 6LoWPAN Working Group, which provides an efficient use of IPv6 over IEEE 802.15.4 networks [15]. The IP-based network not only allows remote access to the devices, but also facilitates the interconnection between different networks, required for building large-scale networks [10]. The normal IPv6 header is relatively large compared to the maximum IEEE 802.15.4 packet size. The header compression and fragmentation are utilized to reduce the header size, resulting in lower overhead for data transmissions, and consequently saving the energy. 6LoWPAN supports unicast, multicast, and broadcast messaging. Hence, the transmitter can choose a specific device, or a group of devices, or all the devices in a network for message delivery. All these features have made the 6LoWPAN popular for developing IP-based networks; it has been implemented in other network stacks, such as ZigBee and ISA100.11a.

ZigBee is a network protocol built on top of IEEE 802.15.4, aimed at providing connectivity for control and monitoring applications. ZigBee alliance is an association of companies working together to develop and maintain the ZigBee standards [16]. ZigBee defines the network, security, and application framework profile layers that enable interoperability between products from different manufacturers. It supports star, mesh, and cluster-tree topologies. Empowered by these network topologies, a single network can cover a large area and accommodate over 65,000 devices [9]. The data transmissions between devices are performed with low-latency without the need for initial network synchronization. However, the reliable communication is not guaranteed as the network operates over a single channel, making the data transmissions susceptible to interference. Hence, a careful channel selection is essential for network planning [17], [18], [19]. The ZigBee alliance ensures the interoperability between devices by providing application profiles, defining message formats, and processing actions. The running applications can interact with devices in the ZigBee networks by the aid of application profiles. The specified application profiles cover building automation, health care, home automation, input device, network devices, remote control, retail services, smart energy, telecom services, and 3D sync. The plethora of profiles have made the ZigBee standards accessible for a wide range of applications.

WirelessHART and ISA100.11a are two major network standards for providing secure, reliable, and low-latency communications using IEEE 802.15.4 [11]. The reliable communications with low-latency is essential for the safe operation of mission-critical applications, such as industrial automation applications. WirelessHART was initially released in 2007 by HART Communication Foundation (HCF) as an extension to the HART Communication protocol. It is a centralized network, in which the whole network is managed by a single network manager. The interconnections of devices and the network manager can be provided by a single AP, known as a gateway, or multiple gateways in case of requiring extended coverage. WirelessHART supports mesh topology, so all the devices can cooperate for delivering data by forwarding packets to other devices in the network. This can reduce the transmission latency and improve the reliability of communications. Data transmissions are performed utilizing time slots, formed by combining time division multiple access (TDMA) with channel hopping. The duration of time slots is fixed at 10 milliseconds (ms). Time slots form a superframe that is repeated over time. The network manager allocates time slots to the devices and gateways in the network according to their traffics. In addition, the channel hopping technique is exploited that alleviates the effects of interference from other networks by switching between channels. Furthermore, the channel blacking technique can be applied. This is an optional feature in which the network administrator can exclude some channels manually from the hopping sequence. WirelessHART ensures the interoperability of the standard with previous and future releases of the HART protocol. So, the new devices can be added to the existing networks without any issue.

ISA100.11a is another standard for industrial automation applications, initially released in 2009 by the International Society of Automation (ISA). ISA100.11a is a centralized network and supports star, star-mesh, and mesh topologies. The routing capability is an optional feature for the devices in the network, enabling utilization of RFD for the end devices. The network employs the combination of TDMA and channel-hopping, with the configurable time slot duration. The channel blacking technique can be performed adaptively, enabling each device to blacklist its desired channels. The ISA100.11a provides a flexible network implementation by allowing to optimize the stack parameters. This flexibility can result in achieving a better performance compared to the WirelessHART. However, it causes interoperability issues between devices from different manufacturers. In addition, the network design is more complex and requires more configurations.

1.3.2 WiFi

IEEE 802.11 standard, known as WiFi, was initially designed for wireless local area networks (WLAN), aiming at providing high data transmission rates for a limited number of connected devices, known as stations, over short distances. The standard has undergone extensive modifications in order to boost the transmission rates. As a result, several IEEE 802.11 amendments have emerged, exceeding the transmission rates to more than 1 Gbps in the latest versions, e.g., 802.11ad and 802.11ac. The amendments define PHY layers over various frequency bands, including 2.4 GHz, 5 GHz, and 60 GHz, with different bandwidths, ranging from 20 MHz to 160 MHz. The high transmission rates have made the standard a prevailing indoor broadband wireless technology in most the countries. The recent IEEE 802.11 amendments are as follows.

- **IEEE 802.11n:** This amendment defines PHY layers operating in 2.4 and 5 GHz bands. The maximum transmission rate varies between 54 Mbps to 600 Mbps.
- **IEEE 802.11s:** This amendment supports mesh networking that can be utilized for extending the network coverage with a limited number of APs [20].
- **IEEE 802.11ac:** This amendment utilizes wider channels in 5 GHz band, which yields the transmission rate up to 1300 Mbps.
- **IEEE 802.11ad:** This amendment defines a new PHY layer in 60 GHz band, which significantly increases the transmission rate up to 7 Gbps. However, the coverage is limited as the frequency band has different propagation characteristics compared to the 2.4 and 5 GHz bands.
- **IEEE 802.11af:** This amendment defines the PHY layer operating in the white space spectrum in the frequency bands between 54 and 790 MHz. The propagation loss in this band is low which improves the communication range, reaching up to 1 km. The maximum achievable data rate is 426 Mbps.
- **IEEE 802.11ah:** This amendment defines the PHY layer operating in the sub 1 GHz (S1G) band. The modifications for PHY and MAC layers address some of the important IoT requirements.

IEEE 802.11 achieves high data rates by utilizing wide channels that are available in high frequency bands, i.e., 2.4, 5, and 60 GHz. The wide-band operation results in making the transceiver expensive and increasing the power consumption, while the coverage is limited due to the high penetration loss. In order to make the standard suitable for IoT applications, IEEE 802.11ah Task Group (TGah), also called low-power WiFi, was formed in 2010. They provide a new amendment by considering the IoT requirements, aiming at improving the transmission coverage, reducing the power consumption, and supporting a large number of stations connected to an AP [21]. The IEEE 802.11ah PHY layer is designed by down-clocking ten times the IEEE 802.11ac PHY layer. In order to achieve an extended coverage range, the IEEE 802.11ah utilizes the S1G frequency band. This band has better penetration properties that increase the coverage up to 1 km without boosting the transmission power. The PHY layer supports different channel bandwidths: 1, 2, 4, 8, and 16 MHz, offering data rates from 150 kbps up to 78 Mbps. This enables balancing the power consumption and transmission rate according to the application demand. The MAC layer adopts various enhancements, including: new compact frame formats, enhanced channel access, improved power management mechanisms, and throughput enhancements. The compact frame formats permit reducing the protocol overheads, consequently resulting in a higher throughput. The traffic indications map (TIM) and page segmentation (PS) are the channel access schemes, which reduce the time that stations need to compete for accessing the channel. The employed hierarchical association identifier (AID) supports up to 8191 stations connected to a single AP, much higher compared to the legacy IEEE 802.11 standard. The new power management modes allow the station to turn off the radio for a long period, while the AP buffers the downlink (transmission from the AP to the device) packets until the station wakes up again. This reduces the power consumption significantly in the station. By employing the mentioned features, the IEEE 802.11ah has become a suitable technology for supporting a wide range of IoT applications for monitoring, smart environment, and industrial automation.

1.3.3 Bluetooth

Bluetooth is a low cost wireless technology for establishing personal area networks (PANs) over short distances, typically less than 100 m. Since 1998, the Special Interest Group (SIG) is responsible for developing and maintaining the Bluetooth open standard. Bluetooth operates in 2.4 GHz, and employs frequency hopping spread spectrum (FHSS) to alleviate the effects of interference. Upto now, five generations of Bluetooth standard have been defined, with the following specifications.

- **Bluetooth V1.0:** The initial version that operates in basic rate (BR) mode with data rate of 1 Mbps.
- **Bluetooth V2.0:** It introduces the enhanced data rate (EDR) mode that provides data rate of 3 Mbps, in addition to support of BR mode.
- **Bluetooth V3.0:** It supports BR mode, with the optional support of EDR mode and high speed (HS) mode that provides data rate of 24 Mbps.
- **Bluetooth V4.0:** It supports BR mode, with the optional support of EDR, HS, and low energy (LE) modes.
- **Bluetooth V5.0:** SIG announced the Bluetooth 5 in June 2016. It will improve significantly the coverage range, speed, and broadcast messaging capacity.

The Bluetooth low energy (BLE), also known as Bluetooth smart, was introduced in 2010 and featured very low power consumption with enhanced transmission range, compared to previous generations [22]. These features have made the BLE suitable for

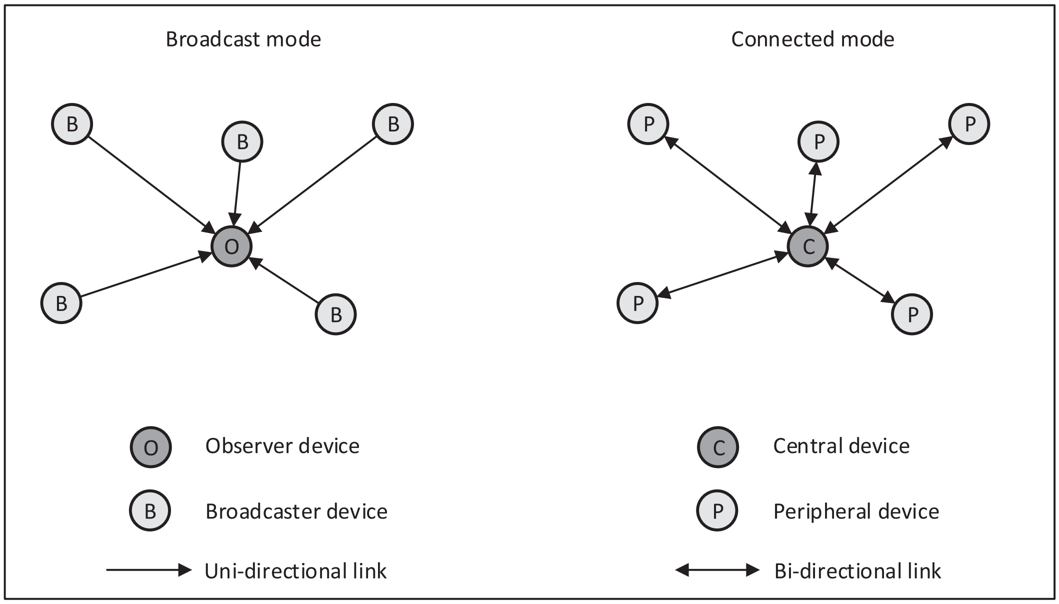

Figure 1.3 BLE communication topologies.

low-power control and monitoring applications. BLE defines 3 advertising channels and 37 data channels, each channel with 2 MHz bandwidth. It employs Gaussian frequency shift keying (GFSK) modulation with increased modulation index compared to the classic Bluetooth, to achieve robust transmission with high coverage and low power consumption [23]. The LE mode achieves data rate up to 1 Mbps. A BLE device can communicate with other devices in one of broadcast or connected modes, as shown in Figure 1.3. The broadcast mode provides unidirectional data transmissions from a broadcaster device to surrounding devices that listen to advertising channels. The data transmissions in the broadcast mode are inherently unreliable due to the lack of acknowledgment feedback. In addition, a limited amount of information can be transferred in this mode. The standard advertising packet contains 31-byte payload. In case the payload is not large enough to fit all the information, there is an optional secondary advertising payload. A scanner device can request the second advertisement frame upon receiving the initial part. Hence, the maximum of 62 bytes can be transferred. The connected mode provides bidirectional data transmissions for a group of devices, forming a piconet. A piconet consists of a central device and one or more peripheral devices. The central device is the master in the piconet and can support multiple connections. The peripheral devices are considered as slaves and are able to communicate only with the master device. In order to join the piconet, a peripheral device broadcasts connectable advertisement messages over the advertising channels. When the central device receives the advertisement message, it can initiate a connection with the peripheral device by sending the connection request. Once the connection is established, the master device and the peripheral device can exchange data over the data channels. Within a piconet, peripheral devices can only communicate with the central device, and not with each other. To reduce the power consumption, the peripheral devices stay in sleep mode by default and wake up periodically to listen for possible packet receptions from the central device. The central device provides the common clock and hopping pattern for the peripheral devices in the piconet. It also manages the medium access by using TDMA scheme and determines the instances that each peripheral device needs to wake up.

BLE includes features that enable achieving very low power consumption, particularly in peripheral devices. This is an important feature for battery-powered devices, such as sensors in health monitoring applications. Studies show that a peripheral device can operate for years while powered with a battery [23]. In addition, a peripheral device can have reduced functionalities. This reduces the design complexity of hardware, while a device can be integrated in a small system-on-chip (SOC). Currently, BLE can be utilized in applications requiring a short-range communication due to the support of single-hop topology. In 2015, Bluetooth SIG formed Bluetooth Smart Mesh Working Group to provide mesh capability for BLE that extends the network coverage [24]. The IoT vision is also considered in the development of Bluetooth v5.0. It is expected that this new release will increase the communication range, the speed of low energy connections, and the capacity of connectionless data broadcast. Employing these features will make the Bluetooth technology applicable for a wider range of applications.

1.3.4 RFID and Ambient Backscattering

Radio-frequency identification (RFID) technologies were initially designed to provide short-range connectivity for the purpose of identification, utilized in various domains such as logistic, manufacturing, health care, security, and access control. Later, a specialized subset of RFID, known as near field communication (NFC), was developed that facilitated the secure data exchange. NFC has been widely deployed in smart mobile devices for performing contactless payment, ticketing, and device pairing. Ambient backscattering is another form of technology that utilizes the ambient radio waves for data transmissions [28]. It is considered as an appealing method of communications for the future smart sensing systems.

RFID enables the unique identification of objects. The objects that are equipped with small tags can communicate with an RFID reader. A reader transmits a query signal to the tags and receives the reflected signals from them. The RFID tags are categorized as passive, semi-passive, and active. The passive tag does not have a source of energy and harvests the electromagnetic energy radiated from the reader for sending response messages. Due to the limited energy, the reading range is short and the tag can only perform very simple computation processes. The semi-passive has a limited access to the power source, mainly for powering the chip while the reader signal is absent. The chip might be connected to sensors for sensing the environment. In this way, the tag can transmit identification information along with the data collected from the sensors. The active tag has access to the source of energy, allowing the support of peripheral sensors and data transmissions over longer distances [2].

Three different frequency bands are allocated for the RFID systems, identified as low frequency (LF), high frequency (HF), and ultra high frequency (UHF) bands. The most common carriers used for LF are the 125 and 134.2 kHz. The LF operation provides low data transmissions over very short range, typically from a couple of centimeters to a couple of meters. The 13.56 MHz band is allocated for HF operation worldwide. It offers higher transmission rates and ability to read several objects at the same time. The UHF systems utilize frequency bands in the range of 300 MHz and 3 GHz, while the 860–960 MHz band is predominantly used. The UHF operation offers the higher data rates, extended range, and ability of reading a larger number of tags simultaneously. The range is limited to several meters for the passive tags [26].

NFC is a bidirectional communication technology based on ISO/IEC 14443 and ISO/IEC 18000-3 specifications [9], [27]. The former specification defines the smart cards utilized for storing information, while the latter specification determines the communication for NFC devices. The NFC devices are categorized as active and passive. A passive device, e.g., an NFC tag, can only provide information for other devices, without the ability to obtain information from others. An active device, can read a passive device and alter the stored information if it is authorized. Additionally, it can exchange data with other active devices. NFC operates in 13.56 MHz band and provides transmission rates ranging from 106 to 424 kbps. The communication range is limited to a few centimeters in order to avoid eavesdropping the data transmissions. An additional level of security is achievable by establishing a secure channel for sending sensitive information. The technology development ensures the interoperability among all NFC products, as well as with other wireless technologies. Nowadays, NFC is embedded in many smart phones to facilitate data sharing and performing payments.

Ambient backscattering takes advantage of existing RF signals, for instance from TV, WiFi, and cellular systems, to harvest energy and perform the data transmissions [25], [28]. It provides communication flexibility, as a device can communicate with all other devices, not exclusively with the readers. The transmitter reuses the ambient signals for conveying the information by changing its antenna between reflecting and non-reflecting states. The reflecting state provides an additional path for the receiver. The receiver distinguishes the transmitter state by assessing the received signals. As the transmitter does not need to have a dedicated source of energy, its size can be reduced significantly. This technology is still in the early development stage; however, it is foreseen that it can be utilized widely in future monitoring systems. For instance, a new type of sensors can be deployed in a home to monitor the environment, while they obtain the energy from the WiFi APs.

1.3.5 Dedicated Short Range Communications

Dedicated short range communications (DSRC) was developed to provide two-way communications, mainly for intelligent transportation systems (ITS) with a wide breadth of applications based on vehicular communications. The envisioned applications have the potential to improve the road safety and utilization [29]. DSRC can support various communication types for vehicular communications, including vehicle-to-vehicle (V2I) and vehicle-to-infrastructure (V2I) communications. DSRC was designed considering the stringent requirements imposed by safety applications, such as low-latency for communications, high reliability, and strict security.

DSRC benefits from other existing technologies [30]. The PHY and MAC layers are based on IEEE 802.11p wireless access for vehicular environments (WAVE), providing data transmissions with a rate of 6–27 Mbps and and a single-hop range of 300–1000 m [31]. The middle layers employ a suite of standards defined by IEEE 1609 Working Group: IEEE 1609.4 for channel switching, IEEE 1609.3 for network services, and IEEE 1609.2 for security services. DSRC supports Internet protocols for the network and transport layers.

A dedicated frequency band in 5.9 GHz is allocated for DSRC operation. Channels have 10 MHz bandwidth and are divided into control and service channels. The control channels are used for the broadcast transmissions and link establishment, while the service channels are utilized for bidirectional communications. Message broadcast is a means for disseminating safety information, including cooperative awareness message (CAM) and decentralized environmental notification message (DENM). The broadcast message is sent without establishing a basic service set (BSS), which eliminates the link establishment latency. However, there are chances for transmission collisions as the channel access is based on the carrier sense multiple access with collision avoidance (CSMA/CA) mechanism.

DSRC still suffers from technical challenges to be widely implemented in ITS. One issue is related to the performance of CSMA/CA in dense networks. The performance of the data transmissions, in terms of reliability and latency, is degraded under high traffic loads. Another concern is related to interoperability of devices. Although the communication protocols are defined, it is not clear how the system can efficiently operate with different applications and in challenging circumstances [31].

1.3.6 Low Power Wide Area Network

Low power wide area network (LPWAN) technologies were developed to provide connectivity for IoT applications that require low-cost device, wide-area coverage, low-power consumption, and exchanging small amounts of data. Such requirements were not efficiently fulfilled with the legacy cellular systems, such as Long-Term Evolution (LTE) Rel-8 and its predecessors. Hence, several preparatory technologies have emerged for enabling LPWAN, including Amber Qireless, Coronis, Huawei's CIoT, Ingenu, LoRa, M2M Spectrum Networks, Nwave, Senaptic, Sigfox, and Weightless [24].

Most of the LPWAN technologies operate in unlicensed bands while utilizing narrow bandwidths. The offered data rates vary across the technologies, ranging from several bps to several hundred kbps. Their coverage ranges can be up to several kilometers, which enable covering very large areas with a limited number of APs. These solutions can achieve low-power consumption while keeping the hardware cost low by featuring simplified functionalities. For instance, an end device may not require performing link establishment and handover in a network. It can send data without establishing a link. Data might be received by multiple APs and are delivered to the cloud-based server. The server then filters the redundant received messages. Another example is the support of single-hop communication that is simple to be implemented, without requiring precise synchronization. In some cases, the transmission latency in download is relaxed, allowing a device to remain in the sleep mode most of the time. The simplified functionalities enable a battery-powered device to operate for several years.

Despite the general similarities in the LPWAN technologies, there are differences in terms of network deployment, operational model, and device categories. The main features for some of the well known LPWAN technologies are as follows.

- **Ingenu:** The On-Ramp Wireless has changed its name to Ingenu. It aims at building a nationwide network. This can accelerate the application deployment as the IoT devices can utilize the network with subscription fee. However, currently only a limited number of countries have the network coverage. The aggregated traffic rates for an AP are limited to 624 kbps and 156 kbps in uplink and downlink, respectively.

- **LoRa and LoRaWAN:** Lora Alliance comprises of different companies participating in the development of LoRa and LoRaWAN. LoRa defines the PHY layer while LoRaWAN specifies the communication protocol and system architecture. The data transmission rates vary according to the communication range and the regional spectrum allocation, ranging from 0.3 kbps to 50 kbps. There are three device classes: one that allows downlink transmissions only during a window period after uplink data delivery; one that permits periodic downlink transmissions; and one that allows downlink transmissions at any time.

- **NWave:** The NWave supports only the uplink data transmissions with the maximum rate of 100 bps.

- **Platanus:** The protocol was designed to support ultra-dense device deployments over modest ranges. The transmission rate can be up to 500 kbps.

- **Sigfox:** This company also aims at deploying a managed worldwide network, currently covering a limited number of countries. The transmission rate is limited to 1 kpbs, with the maximum message size of 12 bytes.

- **Weightless:** It is comprised of three protocols: Weightless-W that is a bidirectional communication protocol operating over licensed TV spectrum; and Weightless-N and Weightless-P, which are narrow-band protocols utilizing unlicensed bands. The Weightless-N supports only uplink transmissions, while Weightless-P provides bidirectional data transmissions. The transmission rates are limited to 100 kbps.

Despite the appealing features of LPWAN technologies, they are faced with some technical challenges, mainly raised from the use of unlicensed bands for long range transmissions. Many countries enforce heavy regulations on utilizing the unlicensed bands in terms of effective radiated power (ERP), duty cycle, and access mechanism [1], [24]. These might limit the transmission rate, the message size, and the number of messages that can be sent over a period of time. Another challenge is related to the asymmetric link performance in uplink and downlink directions, imposed by ERP limitation that is applied at the output of the antenna. The antenna gains for the APs are significantly higher than for the devices, resulting in the better performance in the uplink direction. Consequently, the network cannot effectively control the devices as control information is delivered in the downlink with poor performance. In order to overcome these barriers, some of these technologies, such as Sigfox and Weigthless, are involved with standardization activities to obtain licensed spectrum for the network implementations. The current solutions are able to offer inexpensive connectivity for applications that tolerate the unreliable data transmissions with high latency.

1.3.7 Cellular Systems

The traditional cellular systems, including LTE Rel-8 and its predecessors, were mainly designed to serve human-to-human communications. However, their inherent features, such as wide coverage, easy deployment, access to the dedicated spectrum, and high security level, have attracted many IoT applications to exploit the cellular systems for their connectivity. The fast growth of IoT applications has encouraged the standardization forums to consider enhancements for the cellular systems in order to support IoT applications more efficiently. Consequently, the new releases of LTE encounter new features that facilitate the M2M communications.

The first release of LTE specifications, i.e., LTE Rel-8, was introduced in 2008. The LTE network architecture is fully IP-based that enables accommodating a large set of devices. As shown in Figure 1.4, IoT devices can be connected to the cellular network directly or through gateways [32]. In the direct connection, a device directly interacts with a serving base station, called eNodeB in LTE. This entails that the device be compatible with the cellular air interface. In the indirect connection, a device can benefit from other wired or wireless technologies to be connected to a gateway that acts as a mediator between the cellular network and the device. The indirect connection facilitates the migration of the existing IoT devices to the cellular networks.

LTE Rel-8 defines different user equipment (UE) categories with various performances and capabilities [33]. UE Cat-1 has the basic capabilities and provides data rates up to 5 Mbps in uplink and 10 Mbps in downlink. The achieved transmission rates in basic UE categories are satisfactory for many IoT applications. However, there are several issues that prevent the wide usage of these UE categories for IoT applications. For instance, the price of transceivers is not suitable for low-cost IoT applications. In addition, the transceivers consume a high amount of energy and cannot operate for a long period of time when powered with batteries. Another challenge is related to the network coverage. The transceivers may not operate in locations with high penetration loss, e.g., in a meter closet in which smart meters are generally deployed. In order to eliminate such shortcomings for the wide deployment of IoT applications, The Third Generation Partnership Project (3GPP) has introduced new UE categories, optimized for M2M communications. The first IoT-specific UE

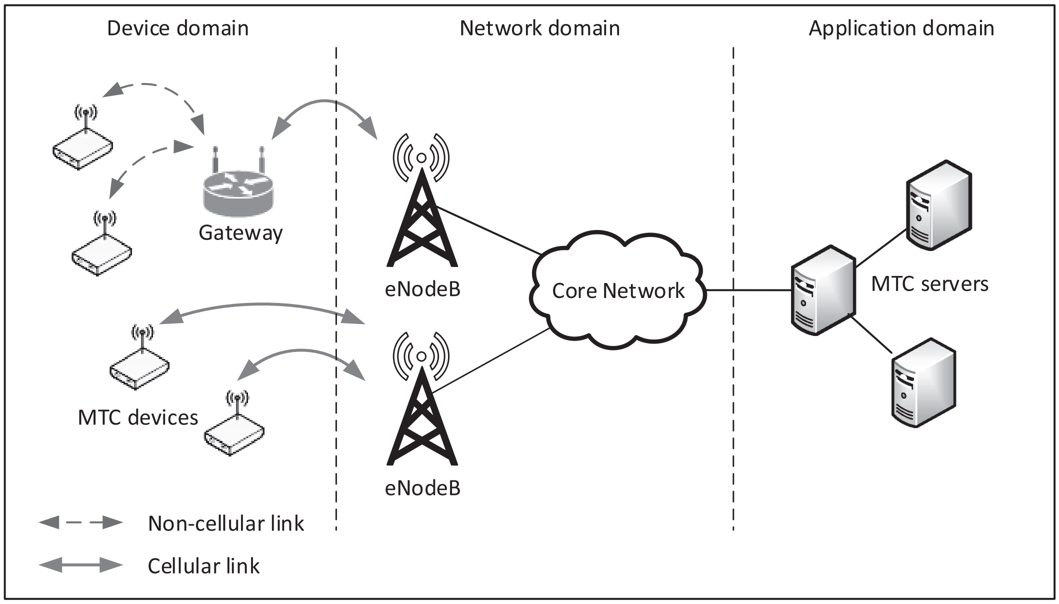

Figure 1.4 M2M communications in a cellular network.

was introduced in LTE Rel-12, known as LTE Cat-0 or LTE-M. This category was enhanced in Rel-13 and appeared as enhanced MTC (eMTC). LTE Rel-13 also introduced another category with narrow-band operation that is called Narrow-band IoT (NB-IoT). Some of the important features for these new categories are as follows.

- **LTE Cat-0:** This is a low-cost MTC UE that operates in 20 MHz bandwidth with the maximum throughput of 1 Mbps in both uplink and downlink. Rel-12 has defined a set of reduced requirements in order to scale down the chip cost and power consumption compared to the basic LTE Rel-8 category, i.e., Cat-1. For instance, Cat-0 incorporates a single antenna, while previous UE categories needed to have at least two receive antennas. This inevitably resulted in reduced coverage and transmission rate due to the loss of receiver combining gain and channel diversity. In addition, Cat-0 has an optional half-duplex operation in frequency division duplex (FDD) mode. This brings further cost reduction by removing the duplexer, as the UE needs to only transmit or receive at a time. With the mentioned reduced capabilities, Cat-0 can achieve approximately 50% cost saving over Cat-1 [34]. In order to reduce the energy consumption, Rel-12 added a power saving mode (PSM) feature to minimize the energy consumption. An UE in PSM mode is basically registered in the network but cannot be reached. It does not monitor the control channels for possible incoming data. So, the data should be buffered in the network side until the UE becomes available, for instance, when it wants to transmit something or when the PSM timer expires. Therefore, data transmission in the downlink may face huge delay, making the PSM mode more applicable for delay tolerant or opportunistic systems, which are not sensitive to delays.

- **LTE eMTC:** This category is based on the LTE Cat-0 featuring additional reduced requirements and coverage enhancements. For instance, the RF bandwidth is limited to 1.4 MHz for both uplink and downlink. The maximum of 1 Mbps data rate can be achieved in uplink and downlink. In addition, the maximum transmit power is reduced to 20 dBm compared to 23 dBm in LTE Cat-1, allowing in integrating the power amplifier (PA) and the radio transceiver in a single chip. The employed features enable to achieve approximately 75% cost saving over Cat-0, making the eMTC more cost-effective. For reducing the power consumption, more advanced discontinues reception (DRX), called enhanced DRX (eDRX), was introduced. A device in DRX mode can avoid monitoring the incoming control information, allowing to save energy by entering the idle mode. LTE Rel-13 specifies coverage enhancements to alleviate the coverage loss due to the reduced capabilities. The enhanced coverage allows to support devices located in places with high penetration loss. The coverage enhancement corresponds to 15 dB improvement for the maximum coupling loss (MCL) compared to the FDD MCL in Cat-0, i.e., 140.7 dB.

- **LTE NB-IoT:** This category was designed to enable: low-cost device, long battery life, high coverage, and deployment of a large number of devices. It inherits basic functionalities from the LTE, while it operates in a narrow band. As shown in Figure 1.5, the NB-IoT has flexible network deployment options: stand-alone, in-band, and guard-band modes. The stand-alone mode occupies a single GSM channel, i.e., 200 kHz. The in-band mode operates over a wideband LTE carrier, while guard-band mode operates out-band of the existing LTE carrier. The occupied bandwidths in both in-band and guard-band modes are equal to the bandwidth of a single LTE physical resource block (PRB), i.e., 180 kHz. The transmission rates are in the range of 100 - 200 kbps. The narrowband operation reduces the complexity of transceiver elements, such as analog-to-digital (A/D) and digital-to-analog (A/D) conversion, buffering, and channel estimation. NB-IoT has the reduced transmission power of 20 dBm. All these features provide cost reduction for the radio chip.

  Another important feature of NB-IoT is the coverage enhancement. The target for MCS is 164 dB, which is almost 23 dB more than the MCL for FDD Cat-0. This provides a good coverage, even for devices located in places with high penetration loss. Additionally, NB-IoT benefits from eDRX for reducing the power consumption, the battery for a device reporting short packets in long intervals can last for up to ten years. It is apparent that NB-IoT covers the important features of LPWAN technologies, while it provides a better performance with access to dedicated radio spectrum.

The new LTE UE categories that are optimized for M2M communications can provide connectivity for a wide range of IoT applications. The LTE Cat-0 and eMTC are suitable for devices requiring high transmission rates, while the NB-IoT is efficient for devices that require long time operation. However, the application deployments depend on the support of new LTE releases by network operators.

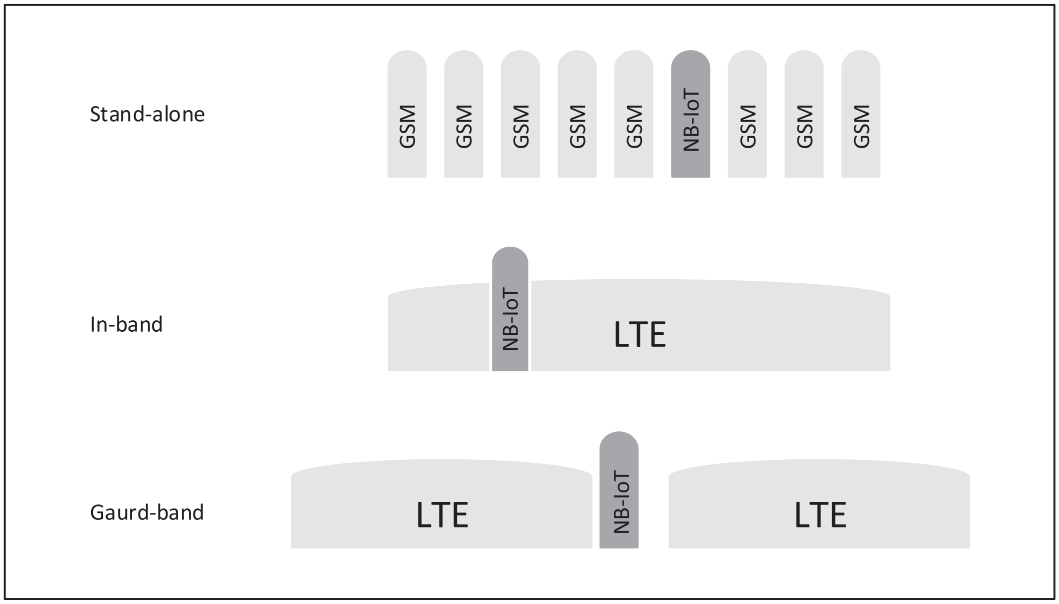

Figure 1.5 Deployment modes for NB-IoT.

1.4 CHALLENGES AND SOLUTIONS FOR CONNECTIVITY IN 5G ERA

Cellular systems are gaining more attention for accommodating IoT applications. The enhancements in the new releases of LTE provide better support of M2M communications. However, these enhancement cannot satisfy all the identified requirements for M2M communications, imposed by the envisioned IoT applications. Thus, further advancements are essential for the future cellular systems, including the fifth generation (5G) of wireless systems, to support M2M communications more efficiently. The rest of this section describes some of the existing challenges that should be addressed, along with some solutions that have been proposed to overcome them.

1.4.1 Low-power Consumption

Power consumption is an important issue for devices that are powered with batteries. In some applications, such as environmental monitoring, the devices are located in areas with limited access. To accommodate such devices in the cellular networks, the low-power consumption mode is essential, permitting a device operates for several years without needing to change the batteries. Some enhancements have been considered in LTE Rel-12 and Rel-13 to reduce the power consumption. Some of the considered enhancements and other possible solutions are as follows.

- **Narrow-band operation:** The narrow-band operation reduces the power consumption and complexity of radio transceiver. The transceiver needs to scan a narrow spectrum, which directly results in lower power consumption.
- **Power saving mode:** This mode was initially introduced in LTE Rel-12 and permits an UE device enters the dormant mode while it remains registered

in the network. A device in PSM mode is not reachable immediately by the network and downlink data should be buffered until the device exits this mode. This is applicable for delay-tolerant applications as the delay in downlink data transmissions can be very high.

- **Discontinuous reception:** This feature enables an UE device stays in the sleep mode without requiring to decode incoming information form the cellular network. LTE Rel-12 introduced eDRX by supporting longer periods that the device can sleep, resulting in saving more energy [35].
- **Supporting multi-hop and group-based communications:** Multi-hop communications can bring power saving for devices located far from the serving base station [36]. Group-based scheme takes the same approach by selecting some of the devices as the gateways in the network. The selected devices collect messages from other nearby devices, aggregate, and deliver them to the network.

1.4.2 Enhanced Coverage

As mentioned earlier, some of the simplified functionalities that are defined for LTE UE categories for reducing the chip cost result in lower signal energy at the receiver. In addition, some IoT devices might be deployed in locations with high penetration loss. In order to overcome these challenges, coverage enhancement techniques can be applied. LTE Rel-12 and Rel-13 introduced some techniques to achieved this goal. Some of employed enhancements in these releases and other possible enhancements are as follows.

- **Retransmission:** Data retransmission, using automatic repeat request (ARQ) or hybrid ARQ (HARQ), can be utilized to ensure the receiver can decode the message correctly. In the ARQ scheme, the receiver tries to decode the message by utilizing received information in the last transmission round, while in the HARQ scheme, the receiver utilizes all the received information to retrieve the message.
- **Transmission time interval bundling:** Transmission time interval (TTI) is the time unit for scheduling uplink and downlink transmissions. In the TTI bundling, several consecutive TTIs are combined to transmit data over a longer period. Hence, data transmissions can be performed with a lower rate, improving the success rate of decoding data.
- **Frequency hopping:** Through the frequency hopping, data can be transmitted over different frequency bands. This scheme alleviates the effects of frequency fading and provides more robust data transmissions.
- **Power boosting and power spectral density boosting:** In the downlink, the base station can increase the transmission power for devices with poor channel conditions. In the uplink, a device can employ power spectral density (PSD)

boosting by concentrating the transmission power on a decreased bandwidth, which results in higher power density over the bandwidth.

- **Relaxed requirements:** Some control channel performance requirements can be relaxed for IoT devices, such as the minimum probability of decoding the random access response.

- **Increasing reference signal density:** The number of resources allocated for reference signal (RS) can be increased to provide better channel estimations.

1.4.3 Ultra-reliable Low-latency Communications

Ultra-reliable low-latency communications (URLLC) refers to provision of a certain level of communication service almost all the time. It is essential for supporting time-critical applications, including: industrial automation, autonomous driving, vehicular safety, and tactile Internet [37], [38]. URLLC implies requirements on the availability, reliability, and latency, according to the applications. For instance, some factory automation use cases need communications with end-to-end latency less than 1 ms with reliability of $1 - 10^{-9}$ [39]. The current wireless solutions, including cellular and non-cellular technologies, cannot meet such stringent requirements. However, cellular systems have a better chance to support URLLC, due to the access to dedicated spectrum. In order to realize URLLC in the future cellular systems, extensive enhancements are required in different parts of the networks, such as device, radio access network (RAN), and core network (CN). The enhancements target at reducing the transmission latency, improving the link reliability, and enhancing the resource utilization. Some of the possible enhancements are as follows.

- **Employing shorter TTI:** LTE defines a frame structure with 10 ms duration. Each frame consist of 10 subframes, which results in having TTI of 1 ms. It is required to employ shorter TTI in order to meet 1 ms end-to-end latency. It is agreed that in 5G, an integer division of 1 ms, e.g., 0.25 or 0.125 ms, would be considered as TTI, at least for delay-sensitive communications.

- **Employing more mode changes in time-division multiplexing:** LTE have two operational mode: time-division multiplexing (TDD) and FDD. In the former mode, downlink and uplink transmissions are occurred in the same frequency band while they are separated in time domain. In the latter mode, uplink and downlink transmissions are occurred over different frequency bands. For TDD mode, different configurations are defined for uplink and downlink subframe allocations. For better support of URLLC, new configurations can be defined to reduce the time gap between uplink and downlink transmissions, e.g., changing the uplink and downlink directions every subframe.

- **Flexible frame structure:** In LTE system, the physical downlink control channel (PDCCH) is located at the beginning of each downlink subframe and it carries control information, including scheduling assignments in downlink and