Chapter 12

An Overview of Network Communication Technologies for IoT

Burkhard Stiller[1], Eryk Schiller[1], Corinna Schmitt[2]

[1]Communication Systems Group CSG, Department of Informatics IfI, University of Zürich UZH
Binzmühlestrasse 14, CH—8050 Zürich, Switzerland
{schiller, stiller}@ifi.uzh.ch

[2]Research Institute CODE, Universität der Bundeswehr München,
Werner-Heisenberg-Weg 39, D—85577 Neubiberg, Germany
corinna.schmitt@unibw.de

Abstract— **This chapter classifies communication technologies employed in the Internet-of-Things (IoT) as infrastructure, data, transport, discovery, messaging, and management protocol families as well as semantics and frameworks. Moreover, IoT networks are divided into IP and Constrained Networks with the latter not directly supporting the Transmission Control Protocol (TCP) and Internet Protocol (IP) stack on IoT devices. Furthermore, another distinction is considered dividing networks into Personal (PAN), Local (LAN), and Wide (WAN) Area Networks. Finally, here selected communication technologies are characterized according to the aforementioned classifiers and important aspects of select technologies are discussed in the remainder of this chapter.**

Keywords— **PAN, LAN, MAN, WAN, IEEE 802.11, IEEE 802.15.4, ZigBee, 6LoWPAN, BLIP, Sigfox, LoRa, DASH7, RFID, NFC, Bluetooth, 1G, 2G, 3G, 4G, 5G, LTE Cat. 0, LTE Cat. M, LTE Cat. M1, LTE Cat. N, NB-IoT, EC-GSM-IoT.**

12.1 Introduction

The Internet consists out of a network of networks connecting differently sized networks, larger ones from full-fledged commercially operated Autonomous Systems (AS) to smaller ones of private or public organizations, via many thousands of different gateways and routers [37]. Each AS itself handles the communication within this AS autonomously. Typically, each constrained network, *e.g.,* a dedicated wireless sensor or an ad-hoc network, defines a single AS-like network connected via a gateway or router to the Internet. Thus, such a constrained network can establish connections to other ASes, *e.g.,* a home or an office network.

The umbrella of constrained networks and their devices — including their interconnections — is often termed as "Internet-of-Things" (IoT), once especially these devices and their data as well as services move into the center of observation (cf. Figure 12.1). In such cases the IoT gateway or router typically has to hold sufficient resources to support the transmission of the traffic received in one constrained network to sent it to any other one. Therefore, and in contrast to many devices, such a gateway within the IoT context is categorized as a "resource-rich" device. Furthermore, device-centric security features, provided by communication protocols in use, determine the basis for secure IoT communications.

12.1.1 IoT Protocol Classification

In case of constrained networks the working infrastructure operates a resource-rich device to interconnect (the "gateway") and coordinate (the "coordinator") that network. Thus, the establishing and managing of the network, the definition of communication technologies to be used internally, and the support of devices selected to connect the network to the outer world can be coordi-

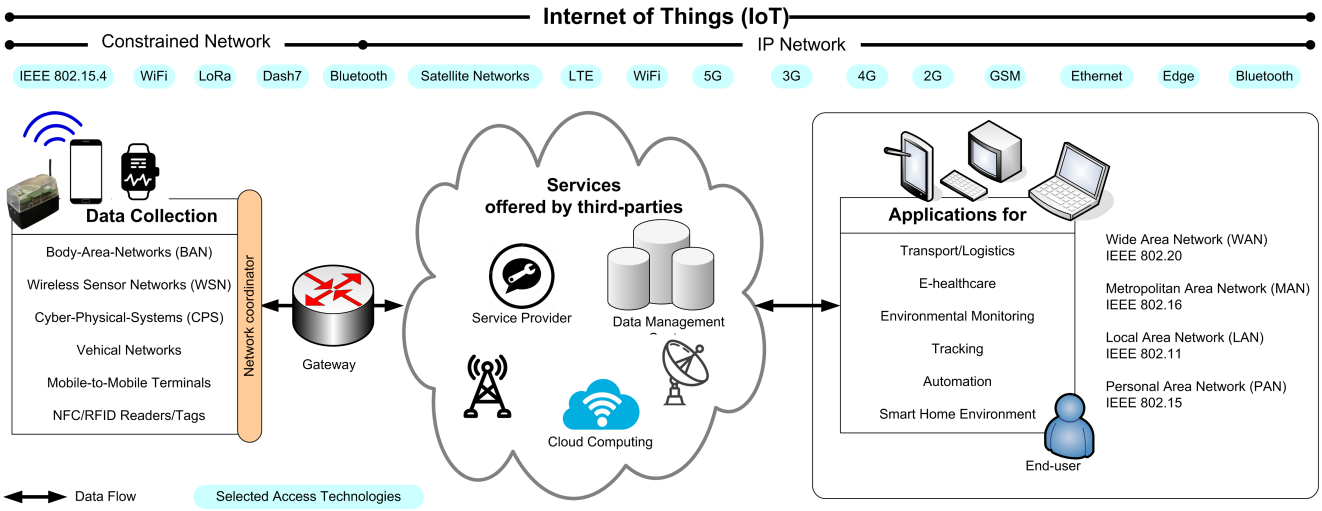


Figure 12.1: Data Flows Within IoT, based on [50] and [18]

nated. Depending on the purpose of this constrained network and on the availability of resources of those devices participating, the network can offer different functionality, such as the communication standard supported, the maximum transmission unit, the maximum number of participants being coordinated, or the services offered.

Since this chapter focuses on network communication technologies for IoT, a classification is required. Although all communications require a Physical (PHY) and the Medium Access Control (MAC) layer protocols, the network layer will be assumed to be operated in an Internet Protocol (IP)-based style. However, IoT communication standards can be classified more precisely by addressing the major task provided [51]. Out of this perspective the focus here will be on (a) the infrastructure perspective with protocols and (b) IoT data communications and transport protocols, however, differently structured according to the physical range of the network. (c) Discovery-related protocols, such as Multicast Domain Name System (mDNS) or DNS-Service Discovery (DNS-SD), (d) messaging data protocols, such as Message Queuing Telemetry Transport (MQTT), Advanced Message Queuing Protocol (AMQP), or Constrained Application Protocol (CoAP) (e) device management protocols, such as Broadband Forum Technical Report 069 (TR-069) or Open Mobile Alliance (OMA)-Device Management (DM), and (f) semantic and framework perspectives, such as JavaScript Object Notation for Linked Data (JSON-LD), Alljoyn, or IoTivity, are all only omitted due to space restrictions.

Thus, *e.g.,* data collected by constrained devices can be transmitted to the outside world by applying the infrastructure perspective and its protocols. To become accessible outside of such a constrained network, the IoT gateway can use interconnections (1) via a private Local Area Network (LAN) (*cf.* Subsection 12.1.3) or (2) via public wireless access communication standards to the public Internet. Since many communication alternatives for IoT devices are wireless in nature, the IoT gateway's major function is to bridge the wireless to the wired environment. Thus, Ethernet-based communications often operate as and toward a backbone for interconnected constrained networks, since this LAN technology in combination with IP provides a reasonably well dimensioned transmission speed for communications, device addressing, respective packet forwarding, and routing mechanisms.

More specifically, IoT data communications and transport protocols interact between (a) IoT devices or (b) those and the IoT gateway. In the Personal Area Network (PAN) and LAN domain they include Institute of Electrical and Electronics Engineers (IEEE) 802.11, IEEE 802.15.4, ZigBee, 6LoWPAN (IPv6 over Low-power Wireless Personal Area Networks), Berkeley Low-power IP Stack (BLIP), Long-Range (LoRa) protocol, Radio Frequency Identification (RFID), Near Field Communication (NFC), and Bluetooth. In the Wide Area Network (WAN) domain they cover cellular networks (1st to 5th generation), such as Universal Mobile Telecommunications Service (UMTS) or 5G, and especially, Long Term Evolution (LTE) for IoT.

12.1.2 IoT Messaging Protocols

Although messaging data protocols will be excluded from an in-depth discussion, their major representatives within the IoT domain include the following ones.

MQTT specifies a messaging protocol to enable monitoring IoT from a remote location [34]. Thus, the ma-

jor task of MQTT is to collect data from IoT devices. In the same line, the Data Distribution Service (DDS) standard by the Object Management Group (OMG) offers a high-performance, expandable, and real-time machine-to-machine message communication, which interconnects constrained devices with the outside, *e.g.,* management or Cloud platforms.

Additionally, AMQP operates message-oriented, too, and was originally designed for middleware environments [33]. Specifically the AMQP IoT messaging protocol processes IoT data within three necessary components, Exchange, Message Queue, and Binding.

CoAP was developed to enable restricted access to IoT devices, which are part of restricted networks, which may include gateways on the Internet and IoT devices [75].

12.1.3 General Network Classification

Due to the fact that the wider umbrella of IoT itself includes many different networks, devices in support of different communication standards, and services depending on the deployment area (*cf.* Figure 12.1), the distinction of major network types should be recalled. [37] distinguishes between:

- Personal Area Network (PAN): small networks used to transmit data between a small number of devices, typically sensors. A subgroup of PANs is defined by Wireless Personal Area Networks (WPAN), which deploy s specific short-range radio communication.
- Local Area Network (LAN): networks interconnecting devices within a limited geographical area, *e.g.,* company or university.
- Metropolitan Area Network (MAN): regional network interconnecting devices across medium-sized geographical areas, such as cities or regions.
- Wide Area Network (WAN): networks extending typically global geographical distances.

Based on this categorization, many IoT communication technologies fall into the category PAN, which are interconnected by LAN communications to the outside world. However, modern IoT devices can interact with wireless WAN standards, such as 5G already, directly.

12.1.4 Chapter Organization

This chapter provides an overview on network communication technologies for IoT, which are used to interconnect constrained networks in various settings. Firstly, the Ethernet in combination with IP is briefly presented in Section 12.2 as the major wired network and inter-networking protocol. Secondly, wireless communication technology alternatives for IoT devices are discussed in Section 12.3, which include IEEE 802.11, IEEE 802.15.4 (embracing ZigBee, 6LoWPAN, and BLIP), LoRa, DASH7, RFID, NFC, and Bluetooth. Thirdly, this view is complemented by cellular communication technology alternatives for IoT devices as discussed in Section 12.4 including the overview on 1G to 5G as standards for public wireless access networks. Fourthly, more specifically the discussion of LTE for IoT is embedded in Section 12.5, which includes details on the 3GPP Release 8, LTE Advanced as 3GPP Release 10, and LTE Advanced Pro with its LTE Categories M and N (3GPP Release 13). Finally, Section 12.6 summarizes this overview on network communication technologies for IoT and draws key conclusions.

12.2 Ethernet and IP

Today's IoT solutions deployed involve communications using Ethernet, especially to interconnect constrained networks to the outside world via an IoT gateway's fixed network interface, and IP, to provide a standardized inter-networking approach for resource-constrained devices and very simple communication end-points, such as sensors.

Ethernet was standardized within IEEE 802.3 [7] initially. It developed further over time supporting higher bit rates and longer distances by moving from twisted pair to fiber optics. While each participant is assigned an individual Medium Access Control (MAC) layer address, the direct addressing of devices for sending and receiving Ethernet frames is possible. These frames may have to be split into fragments, which are error-checked, too. At the intended destination, the frame is analyzed to detect damaged frames and in case of need they are discarded. During the starting phase of the early Internet the number of participating devices was manageable via MAC addresses.

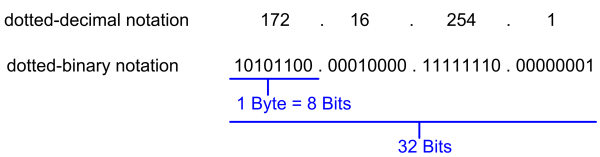


Figure 12.2: IPv4 Address Format [49]

However, as the number of devices grew, the addressing of devices across a larger geographical range could not be handled by Ethernet's MAC addresses anymore. Thus, the address space offering as many as 2^8 addresses in 1974 [19] was exhausted within less than 10 years, thus, new IP version 4 (IPv4) — now focusing on the

network layer above the MAC layer — supported an address range of 2^{32} addresses [49]. IPv4 addresses are 32 bit long and follow regularly the dotted-decimal notation consisting of four octets (*cf.* Figure 12.2). Even this address space became to small, thus, in 1998, IP version 6 (IPv6) was released supporting 2^{128} addresses [57]. These IPv6 addresses are 128 bit long, consisting of a 64 bit prefix and a 64-bit Interface ID (IID). The prefix part identifies the network a device belongs to. The IID identifies the network interface and must be unique for the network.

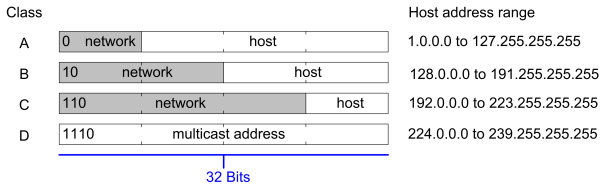


Figure 12.3: Class-based Splitting of IP Addresses [16]

Addressing is the key for devices to be uniquely be identifiable and traffic to and from these to be routable. Thus, while the IPv4 address was divided into two parts initially (the network identifier and the host identifier), this separation supported only 256 network identifiers and turned inadequate over time due to many more devices added to the Internet. Therefore, the network identifier was redefined into network classes, where each class became determined by the bit length of the network identifier. This setup resulted in classes (*cf.* Figure 12.3), but fixed classes caused a waste of addresses. As a result, the Classless Inter-Domain Routing (CIDR) was introduced [27] allowing to assign IP addresses in those amounts needed for individual networks. Therefore, the resulting network size was very flexible and could be adapted to basically any number of devices — well suited for IoT-based constrained networks. Thus, this IP-based addressing forms the basis for all IoT communications, which are exploited with different protocols as the following sections show.

12.3 Wireless PANs and LANs

Wireless accessibility is important for end users and is needed for many devices (*cf.* Figure 12.4), as backed by [22], [30]. In general, wireless networks use radio communications on different frequencies depending on their availability and on the distance to communicate through. To connect to the world, networks operate a "base station"—the gateway to a backbone network. Wireless communication technology examples include (a) cellular networks, *e.g.,* GSM (Global System for Mobile Communications), UMTS, or LTE (*cf.* Section 12.4), (b) wireless LANs and PANs, *e.g.,* IEEE 802.11 and IEEE 802.15.4 (*cf.* Subsections 12.3.1 and 12.3.2 below), (c) various dedicated Wireless Sensor Networks (WSN) for monitoring, logistics, or agriculture, (d) satellite communication networks for navigation and broadcast services, or (e) terrestrial microwave networks.

Today, resource-rich devices in the IoT context vary with respect to the wireless communication technology applied, covering communications for rice-grain sized devices to satellite or aircraft-sized objects. These devices themselves support various functionality, such as data collection, localization, or data exchange. Since industrial solutions as of today need to inter-operate with more than a handful of different wireless technologies, many wireless technologies have turned into a standard describing the PHY and MAC layers. However, these standards differ with respect to their signaling methods, geographic ranges, and frequency use specified. Therefore, certain technologies are better suited to PANs, while others are better suited for larger deployments in MANs or WANs. The following subsections focus on PAN and LAN standards used for constrained networks. Depending on the resources available in a constrained network, additional components and a connection to cellular networks may be required.

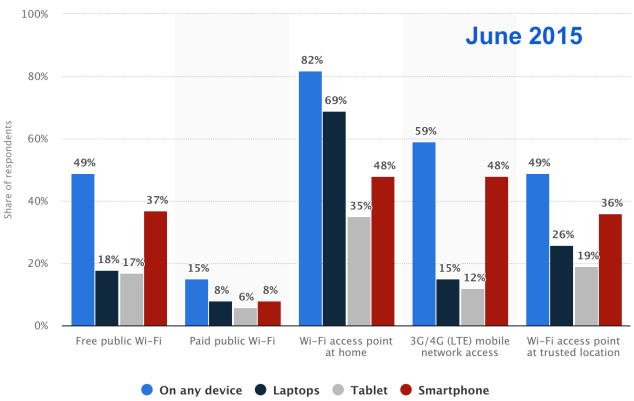


Figure 12.4: Wireless Internet Access by Device According to Internet Users Worldwide [70]

12.3.1 IEEE 802.11

For a straightforward and simple interconnection of IoT devices in a local network's range the WLAN-based approach can be deployed. This offers a quite simple and robust solution for time-bounded and asynchronous services in which a MAC layer interfaces with multiple PHY layers using different medium senses and transmission characteristics. The IEEE 802.11 standard [6] specifies the PHY layer and the MAC layer, while sup-

porting inter-operability to higher layers. Further requirements important for the IoT context include energy efficiency and a worldwide operability, which was achieved by agreeing on using the licence free 2.4 GHz ISM (Industrial, Scientific, and Medical) band. Data rates up to multiple hundreds of Mbit/s per access point have been reached up today.

Theoretically, IEEE 802.11 offers (a) an infrastructure-based architecture as used for IP networks and WSNs or (b) an ad-hoc architecture deployed within Mash Networks (MANET) or Vehicular Ad-hoc Networks (VANET). In both cases, communication is supported by IEEE 802.11. Any application on an IEEE 802.11-compatible device communicates with other devices with differences in terms of bandwidth and access times. While the detailed description of the PHY layer and MAC layer can be found in the standard [6], the following characteristics are to be highlighted with respect to IoT devices. The PHY layer consists of two parts, while being responsible for the channel tuning:

- Physical Layer Convergence Protocol (PLCP): provides the carrier sense signal, termed Clear Channel Assessment (CCA) and a common PHY layer service access point independent of the transmission technology used.
- Physical Medium Dependent (PMD) sublayer: being responsible for modulation and encoding/decoding of signals.

The MAC layer is responsible for the medium access, the fragmentation of data, and the encryption used. This includes the access control management for the association and re-association of devices to an access point and roaming between several access points, including the authentication mechanism, the encryption, a synchronization of devices in the network, and a power management to enable an energy efficient device operation. Thus, due to the more heavy-weight layer specification and its implementation only resource-rich devices from am IoT context can benefit from IEEE 802.11 communication services.

12.3.2 IEEE 802.15.4

For IoT devices in a personal network's range, the IEEE 802.15.4 standard was especially developed for WPANs [32]. Since it does respect the standard header sizes of IP and Transmission Control Protocol (TCP), it had become a common standard for IoT devices. This is especially important, since normally a Maximum Transmission Unit (MTU) of 1280 Byte for IPv6 is too large for low-powered devices providing MTU sizes of 127 Byte only. Therefore, IEEE 802.15.4 supports two different device types, distinguished by resources available: (a) "Reduced Functional Device" (RFD) and (b) "Full Functional Device" (FFD). RFDs typically show lesser resources, when the IoT setup needs to operate sensor nodes, Radio Frequency Identifier (RFID) tags, or actor, which typically collect data periodically, establish connections to FFDs, transmit data, and receive data from time to time. In order to save resources, especially energy, those devices support "sleep modes". In contrast, FFDs as a resource-rich device coordinate a network, synchronize network participants, (pre-)process data, and communicate with RFDs as well as other FFDs.

IEEE 802.15.4 defines the PHY and MAC layer only, no functionality for the classic network layer is supported. Thus, all network layer services must be provided by higher layers or special protocols. Work in the IoT domain resulted in the development of different approaches for constrained devices in support of routing, *e.g.,* ZigBee, 6LoWPAN, BLIP, RPL [75], or Hydro [23] (*cf.* Subsection 12.3.3), which include standardized interfaces. This principle followed by IEEE 802.15.4 ensures inter-operability between different implementations.

The PHY layer supports radio communications on different frequency bands, *e.g.,* 868/915 MHz in Europe and the US, 2.4 GHz worldwide). Interference resistance is achieved by supporting the Direct Sequence Spread Spectrum (DSSS), which spreads each outgoing signal with one pre-defined bit sequence [60]. Alternative transmission modes have been added to the PHY layer to provide modern insights in advanced modulation techniques, too.

The MAC layer offers two transmission modes: (a) unslotted mode and (b) slotted mode. Within the unslotted mode, each participant checks, whether the communication channel is free before sending by applying Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA) algorithms. If the medium is free, the transmission starts, otherwise the device waits for a random time slot and tests the channel again. In order to ensure that a transmission was successful, an acknowledgement mechanism may be supported. The unslotted mode does not request any coordination of the network coordinator at all.

IEEE 802.15.4 offers access control, confidentiality, frame integrity, and sequential freshness. Security functionality on the MAC layer is reached via message integrity checks and encryption. While keys used are distributed and administrated by the MAC layer, the explicit encryption is performed by each communication partner and applied by the MAC layer. However, optional features can actually reduce the security level

IEEE 802.15.4 offers.

12.3.3 IoT Network Layer Protocols

Under the assumption that constrained networks should inter-operate with IEEE 802.15.4-based systems, major IP functionality needs to be supported, especially IP addressing. However, constrained resources do not allow for a direct implementation of the TCP/IP stack on an IoT device. Therefore, resource-efficient solutions and protocols for constrained networks include protocols for WSNs, especially ZigBee, 6LoWPAN, and BLIP.

ZigBee

The ZigBee-Alliance based on IEEE 802.15.4 developed the ZigBee stack (*cf.* Figure 12.5a) supporting IP communication for resource constrained hardware [78]. The ZigBee stack requires 8 kByte RAM, produces 8 to 16 Byte of network overhead, and can support a mesh functionality. The maximum network size counts 1024 nodes participating within a communication range of up to 200 m. While the full protocol stack includes the PHY layer (at 868 MHz, 933 MHz, and 2.4 GHz with a data rate of 250 kBit/s) and MAC layer from IEEE 802.15.4, the overall energy efficiency is reached by placing functions within the MAC layer. On top of the ZigBee part the following function set was added [24]:

- The network supports network scan, network creation or joining, device and service discovery, binding, addressing, and routing. It offers security essentials, such as the 128 bit AES (Advanced Encryption Standard).
- The application layer comprises:
  - ZigBee Device Objects (ZDO): responsible for discovering new devices and their provided services, assigning individual ZigBee profiles to each devices, initiating or responding binding requests, and support security related tasks.
  - ZigBee Application Support Sub-Layer (APS): creating binding relation tables including information of services offered, managing group addresses, mapping 64 bit addresses to 16 bit networking addresses, and supporting reliable data transport.
  - Application Framework: in support of interoperability between devices requiring different application profiles.
- The application profiles layer is responsible for specifying unique device descriptions including functionality required, attributes demanded, and identifiers. These profiles conform to any of the two groups: Private profiles are defined by the device's manufacturer and public profiles are defined, developed, and maintained by the ZigBee Alliance.

Finally, applications are located on top of the ZigBee stack part and contain user-specific protocols [78].

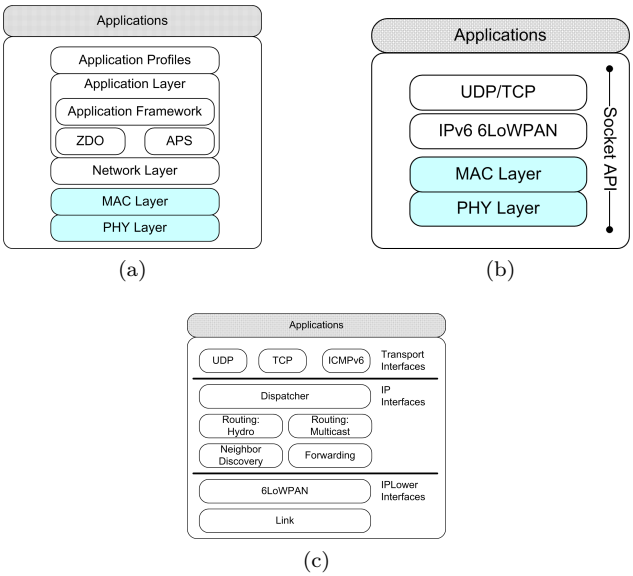


Figure 12.5: Stack Comparison: a) ZigBee Stack, b) 6LoWPAN Nano Stack, c) BLIP Stack [62]

6LoWPAN

The Internet Engineering Task Force (IETF) established working group 6LoWPAN (IPv6 over Low-power Wireless PAN) [65]. A 6LoWPAN implementation offers IPv6 features on top of User Datagram Protocol (UDP)/TCP to sensor nodes regardless of the underlying PHY layer and the 6LoWPAN nano stack only requires 4 kByte RAM. As a result, RFC 4919 [38] presents an overview, assumptions, the problem statement and goals of 6LoWPANs, RFC 6282 [31] specifies the transmission of IPv6 packets over IEEE 802.15.4 networks, RFC 6606 specifies routing [36], RFC 6775 addresses neighbor discovery [66], and RFCs 8055 and 8025 define header handling strategies [20, 71]. Thus, interoperability with IP networks was reached.

Especially, the 6LoWPAN nano stack developed (*cf.* Figure 12.5b) consists out of a Socket API (Application Programming Interface) and applications, which are addressed via socket interfaces. The Socket API is build by the following components [29]:

- PHY: based on IEEE 802.15.4, supports basic radio communication capabilities.

- MAC: based on IEEE 802.15.4, supports contention-based channel access method of unslotted CSMA/CA for data transmissions.
- Network layer: replaced by an adaptation layer 6LoWPAN supporting compression of TCP/UDP and IP headers with 2 to 11 Byte overhead only, packet fragmentation, reassembling, routing, neighbor discovery, and multicast support.
- Transport layer: supporting UDP and TCP.

6LoWPAN supports a 16 bit and 64 bit address space, different bandwidths, and network topologies with a maximum number of 264 devices, and offers an AES 128 encryption and authentication on the link layer.

Finally, applications located on top of that stack are linked with specific interfaces to support user-specific functionality. Thus, ZigBee makes IP communication feasible for constrained devices, especially for those with a limited MTU site of 102 Byte on the MAC layer.

Berkeley Low-power IP Stack (BLIP)

Efficiency advantages of 6LoWPAN compared to ZigBee drove the development to shrink even further the required space for a full stack. A 6LoWPAN version compatible with TinyOS was called Berkeley Low-power IP stack (BLIP) [17] and supports different constrained device platforms with the RF transceiver CC2420 from Texas Instrument, *e.g.,* IRIS and TelosB, which is an IEEE 802.15.4-compliant radio transceiver supporting the MTU of 127 Byte [21]. The streamlined BLIP stack consists of the parts as illustrated in Figure 12.5c [68]:

- IPLower Interface: link layer support is included with a 6LoWPAN layer on top, 6LoWPAN component compresses headers and breaks large packets into multiple link-layer fragments to compile with the MTU used.
- IP Interface: offering network functionality, such as IPv6 neighbor discovery, forwarding, routing (default selection, point- to-point), and dispatching.
- Transport Interface: supporting standard UDP and TCP protocols.
- Applications: including all relevant user protocols and algorithms.

BLIP always provides a tunnel for connecting the gateway to the outside world. Thus, since BLIP offers addressing, stateless auto-configuration, different header compression features, and similar security features as 6LoWPAN, BLIP enables IP communications for constrained devices.

Sigfox

The Sigfox Protocol [67] was developed and designed for Machine-to-Machine (M2M) applications. As a proprietary protocol, backed by a number of Hardware developers, it employs the Differential Binary Phase-Shift Keying (DBPSK) and the Gaussian Frequency Shift Keying (GFSK) as the modulation scheme to work on the ISM band. The wide-reaching signal Ultra Narrowband (UNB) in use passes freely through solid objects and requires little energy, thus, Sigfox belongs to the Low-power Wide-area Network (LPWAN) class. Since the network follows a one-hop star topology, it requires a cellular network access via a gateway to carry the generated traffic to the outside world. Sigfox reaches data rates up to 1,000 bit/s for which only 50 mW of power are needed. Interesting to note is the fact that the UNB signal easily covers large areas and can reach underground IoT devices. Similarly to the LoRa approach and The Things Network (*cf.* 12.3.4 below), the Sigfox IoT network is commercially operational in a number of countries.

12.3.4 LoRa

The LoRa (Long-Range) communication is a closed proprietary product belonging to Semtech, which offers an energy-efficient, secure, and affordable radio technology used in so-called Long-Range Wide Area Networks (LoRaWAN). Due to the closed protocol situation, no paper completely summarizes the current details of LoRa.

LoRaWAN was specified by the non-profit organization LoRa Alliance with more than 428 Members, *e.g.,* Swisscom, Orange, Semtech, Bosch, Cisco, IBM, and Libelium, all over the world [41]. LoRa uses frequencies within the license-free ISM-band (Europe 433/868 MHz, USA 915 MHz, and Asia 430 MHz). The communication is nearly free of interference, since frequency spreading is applied. The communication range varies between 2 to 15 km depending on the environment, however, LoRa proves even a successful signal reception from a low orbit satellite [4]. The main advantage of LoRa is its sensibility of -137 dBm, allowing for a deep penetration into buildings, thus, increasing network availability. LoRa devices and gateways communicate with each other using different channels with data rates ranging from 0.290 to 50 kbit/s. To allow for an energy-efficient operation the Adaptive Data Rate (ADR) shall be provided on every end-device.

LoRa Device Classes

Communications in a LoRaWAN are always separated into Uplink (UL) and Downlink (DL) communications.

While the UL relates to the communication from an end-device to the gateway, the UL reached an end-device. LoRa specifies three classes of devices [69]:

- Class A ("All") are devices usually charged with batteries. Normally, they reside in a sleep mode and are only activated upon sending. UL messages can be originated at any time, *i.e.,* the protocol follows the pure ALOHA design [12]). The UL is only allowed during two consecutive reception windows opened directly after an UL transmission.
- Class B ("Beacon") devices are similar to their counterparts in Class A, but include additional reception windows synchronized to beacons originated by gateways.
- Class C ("Continuous") devices may almost always receive UL messages, with the exception of an ongoing UL transmission on the end-device. Hence, such an operation is power-hungry.

LoRaWAN Network Architecture

All LoRa-enabled devices use the LoRa MAC protocol, which supports distinct applications running on top. "The Things Network" (TTN) uses LoRaWAN to provide its services, *e.g.,* device management, application management, duplicate filtering, or payload reception and presentation [9]. LoRa end-devices collect data, *e.g.,* location information or environmental data, and transmit them as a LoRa transmission to a gateway (*cf.* Figure 12.6. The transmission may be received through multiple gateways at the same time, since end-nodes are not attached to any particular gateway. When a gateway receives a LoRa packet, it forwards the packet over the Internet to the Network Server. The TTN receiving the data, releases it toward the end-user using an API. These data become available for authorized users only. The TTN stores these data received only for a limited amount of time allowing end-users to store the data on a third-party storage service in the network, *e.g.,* a standalone server) [18]. Users can run multiple applications receiving and processing the data for their own purposes such as tracking, monitoring, or data analysis.

Modulation

Since the ISM band is located in Europe and the US in the 902-928 MHz and 863-870 MHz bands, LoRa signals in the ISM band are composed of so called chirps modulated using the Chirp Spread Spectrum (CSS) technique [56]. Additionally, the typical LoRa Bandwidth (BW) is 500 kHz and 125 kHz in North America and Europe, respectively.

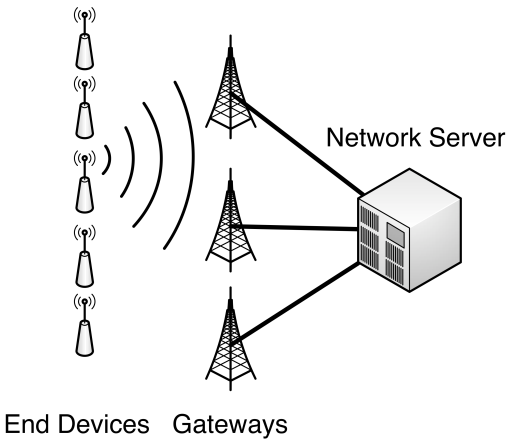


Figure 12.6: LoRaWAN Network Diagram



Figure 12.7: The Authors' Recording [58] of an UL Transmission by an Arduino (Atmel AVR) Node [3] Equipped with a LoRa Shield [2] Presented in Inspectrum [72]

Thus, Figure 12.7 displays an example UL LoRa transmission sent from an Arduino-based node equipped with a LoRa shield based on regular SX1276/SX1278 transceivers. The signal presented consists of *up-chirps* and *down-chirps* spread among the available channel. Up-chirps start with a signal of low frequency and increase the frequency over time, while down-chirps (or conjugated chirps) start with the signal of a high frequency and decrease the frequency over time (*cf.* Figure 12.7). For example, in Europe, assuming the center frequency of 868.5 MHz and 125 kHz BW, an unmodulated up-chirp (respectively down-chirp) would linearly change its frequency between 868.4375 MHz and 868.5625 MHz in time. The UL signal begins with a so called preamble consisting of 10 unmodulated up-chirps. Those are then followed by two and "a quarter" unmodulated down-chirps that point out the end of the preamble and indicate the subsequent payload. The payload consists of symbols coding the header, the message, and a Cyclic Redundancy Check (CRC) used for final error detection. The unmodulated up-chirp is defined in the time-domain using the following formula [56]:

$$\phi_{up}(t) = A \exp\left[i\left(\phi_0 + 2\pi\left(f_0 t + \frac{k}{2}t^2\right)\right)\right], \quad (12.1)$$

where A is the signal amplitude, i is the imaginary unit, ϕ_0 is the initial phase of the signal, f_0 is the lower frequency bound $f_0 = -\frac{BW}{2}$, $T_S = \frac{2^{SF}}{BW}$ is the chirp dura-

tion [5], SF is a so called Spreading Factor (SF), and k is the frequency change coefficient $k = \frac{BW}{T_S}$. The unmodulated down-chirp is produced using the complex conjugate (c.c.) of the unmodulated up chirp: $\phi_{down}(t) = \phi^*_{up}(t)$. A varying SF (*i.e.*,, $SF \in \{7 \dots 12\}$) influences the air-time, when keeping the packet size and BW constant. The higher the SF, the longer the time on the air; higher SFs typically mean longer range, *i.e.,* $SF7$ and $SF12$ have the shortest and the longest range, respectively. It is also worth noting that increasing SF by 1 doubles the symbol duration, while the spreading factors are orthogonal to each other, meaning that signals with different spreading factors do not interfere with one another. This is a so called Code Division Multiple Access (CDMA) property, in which a shared medium is adapted for multiple access from concurrent terminals.



Figure 12.8: The Authors' Recording [58] of a DL Transmission by a LoRa Gateway Node towards Arduino (Atmel AVR) Node [3] Equipped with a LoRa Shield [2] Presented in Inspectrum [72]

To produce a UL LoRa signal, the modulator flips all down chirps up and vice versa, *i.e.,* using the c.c. of the regular LoRa UL signal. Please notice the effective preamble consisting of 10 down chirps, followed by 2.25 up-chirps, which precedes the message only encoded with down-chirps (*cf.* Figure 12.8).

As an example (*cf.* Figure 12.9), three symbols are modulated in the $BW = 125$ kHz, $SF = 7$ LoRa setup. The first symbol is an unmodulated chirp, while the second and third symbols are modulated with a value 32 and 64, respectively. A modulated chirp is based upon a quantized time-shifting (max 2^{SF} states) of the unmodulated chirp. It, therefore, encodes SF bits and is modulated by playing the unmodulated chirp in advance, where the time shift (*i.e.,* advance) for the SF-long bitstream $b \in \{0 \dots 2^{SF} - 1\}$ is quantized and defined as $\hat{t} = b \times \frac{T_S}{2^{SF}}$ (*cf.* Figure 12.9a). When the upper bound frequency is reached after $T_S - \hat{t}$, the modulator restarts with the beginning of the unmodulated chirp to fill out the remaining part of the symbol, *i.e.,* $[T_S - \hat{t}, T_S]$. As a consequence, *cf.* Figure 12.9b, the modulated chirp starts with a signal of a little bit higher that f_0 initial frequency, *i.e.,* $f_0 + BW \times \frac{b}{2^{SF}}$, continues until the upper frequency bound $f_0 + BW$ is reached, and restarts with f_0 until the initial frequency $f_0 + BW \times \frac{b}{2^{SF}}$. Effectively, there are 2^{SF} frequency bins called chips, *i.e.,* $\forall_{b \in \{0 \dots 2^{SF}-1\}} : f_0 + BW \times \frac{b}{2^{SF}}$, coding SF-long bitstreams.

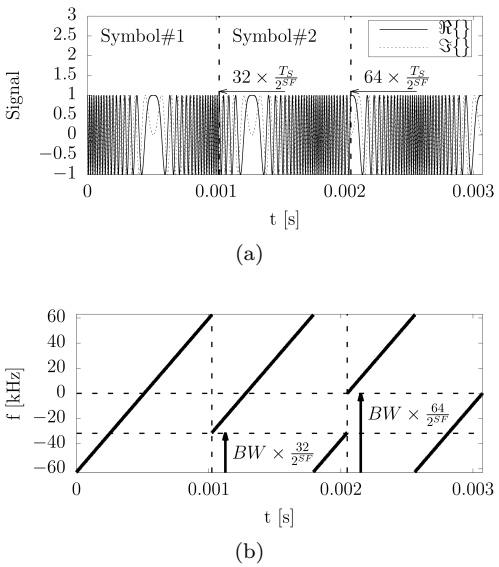


Figure 12.9: LoRa Modulation: a) An Example Modulated Signal in Time, b) Frequency Change of the Modulation in Time

The bit rate R_b is evaluated by $R_b = SF \times \frac{[\frac{4}{4+Cx}]}{[\frac{2^{SF}}{BW}]}$, with Cx being the coding rate for the error correction scheme [1]. Therefore, an elevated coding rate lowers the bit rate, as with the higher Cx, more redundancy is added by the error correction scheme. In the case of $BW = 125$ kHz, the highest data rate of 5.5 kbit/s and the lowest data rate of 0.290 kbit/s is is achieved with $Cx = 1$ and $SF7$ as well as $Cx = 4$, and $SF12$, respectively. The link budget is estimated at 155 to 170 dB (https://blog.semtech.com/title-10-things-about-lorawan-nb-iot).

Coding, Whitening, and Interleaving

LoRa signals are encoded to channel with a modified Hamming coding [56] of a given coding rate (CR), where CR denotes the fraction of data carrying the actual information. The channel code provides reliability to noise by introducing redundancy, which results in a longer binary sequence. There are four different coding schemes, $Cx \in \{1, 2, 3, 4\}$, resulting in different $CR = 4/(4+Cx)$. Coding acts on data nibbles (*i.e.,* 4 bits) producing longer sequences of $4+Cx$ bits. For example, for $Cx = 1$, 4/5 of data is the actual information, while remaining bits are used for error correction [5]. The higher the Cx (*i.e.,* 1-4), the largest amount of corrupted information can get successfully corrected by Forward Error Correction (FEC), however, more redundant bits need to be transmitted as well. It is worth noting that the header is always encoded with the highest coding rate, $Cx = 4$,

because the header contains crucial transmission information such as the message coding rate or packet length. However, a channel coder also introduces bit correlations in the resulting binary sequences.

To remove the correlation, the whitening procedure is used, which calculates the binary eXclusive OR (XOR) function over the binary data encoded and known sequences possessing good statistical properties [44] to improve the randomness of the data stream. Subsequently, the inter-leaver scatters the coded and whitened sequence in time to improve burst error correcting capacity of the signal impacted by the impulsive noise. LoRa uses a diagonal inter-leaver that makes sure that an entirely corrupted chirp only affects one bit per code word, which can be easily recovered by the FEC mechanism. To this end, an $SF \times (Cx + 4)$ matrix is delivered filled by SF codewords row by row. The resulting matrix is then rotated upside-down, circularly shifted downwards using the column index, and transposed resulting in a $(Cx + 4) \times SF$ matrix.

Finally, chirps are modulated using the Gray transformation of the resulting SF-long bit-words received from the received matrix row by row. The reason for Gray coding is that adjacent symbols encoding binary values differ in only one bit. Therefore, small chip detection errors (*e.g.,* ± 1) can be efficiently corrected by FEC.

12.3.5 DASH7

The DASH7 Alliance (D7A) protocol [53] is an active RFID alliance standard for 433, 868, 916 MHz wireless sensor communications based on the ISO/IEC 18000-7 standard. ISO/IEC 18000-7 defines parameters of the active air interface communication.

D7A [74] builds upon an asynchronous WSN MAC. DASH7 provides multi-year battery life, range of up to 1-2 km, low latency for connecting with moving things, a very small open source protocol stack, and the AES 128 bit shared key encryption support. The standard depends on the Gaussian Frequency-Shift Keying (GFSK) modulation and supports the communication capacity of 13 - 200 kbit/s using 4 - 16 channels. The architecture of DASH7 resembles LoRa, in which the End-Devices (ED) connect to Gateways (GW) to report data towards a Network Server (NS), however, DASH7 uses CSMA/CA as the medium access technique.

12.3.6 Radio Frequency Identification

Radio Frequency Identification (RFID) is standardized within the ISO/IEC 18000 series [8]. The original idea was to tag objects allowing to register and track them when passing a special reading device. Therefore, electromagnetic fields are used. These tags are passive devices containing electronic information about the object (*e.g.,* name or product number). Normally, those tags are passive devices requiring energy from nearby reader's to interrogate with them, but not being directly under them unlike barcodes. For successful readings a distance of a few centimeters is assumed. In case they need to be read from further distance, *e.g.,* some hundred meters, the tags require a local power source and are called active tags in turn. RFID tags usually operate on different ISM bands depending on national regulations. The most common ones used for passive tags include [64, 73]:

- 13.56 MHz for communication distance between 10 cm to 1 m
- 865-868 MHz in Europe and 902-928 MHz in North America for a distance of 1-12 m
- 433 MHz for a distance of 1-100 m

For active tags usually 2,450-5,800 MHz are used supporting distances between 1 to 2 m and it is envisioned to use also the ultra-wide band 3.1-10 GHz for communication up to 200 m. Over the decades properties of RFIDs developed further and signaling developed depends on the frequency used (*cf.* ISO/IEC 18000 series [8]). RFID tags can respond to radio signals, store additional information, and can comprise smart-card capabilities with simple processing power.

The original idea of tracking items still holds today, but the application area became broader together with the emergence of IoT together with the cheap development possibilities of active tags [55, 25]. Today, RFID tags can be attached to clothing or personal items, *e.g.,* bikes, drawings, inventory, or can be implanted in bodies. Especially the latter usage raised privacy concerns [35] and, thus, standardization happened addressing this issue. For example, the standards ISO/IEC 18000 and ISO/IEC 29167 specify methods to make devices untraceable by using on-chip cryptography and to support tag and reader authentication [8]. In order to support authenticity, the ISO/IEC 20248 standard specifies digital signatures for RFIDs.

Z-Wave

In the context of low-power RFID communications a typically used protocol is termed Z-Wave, which supports home automation applications [77]. Thus, sensors, lamp, shutter, and blind controllers determine in a smaller geographical distance the set-up, which offers low latency communications and is shielding from other

wireless technologies. Z-Wave IoT protocols are implemented as a proprietary system on a chip (now standardized and maintained by the Z-Wave Alliance) and use the sub-1 GHz band, especially between 856 to 926 MHz, are easily configured and setup as a source-routed mesh network architecture, and the physical range covers up to 100 m. They provide Cloud access via a gateway, the Z-Wave bridge. Data rates achieves so far are between 40 and 100 kbit/s. The interoperability of Z-Wave is reached at the application layer only, since IoT devices can share information and allows all Z-Wave hardware and software to interoperate.

12.3.7 Near Field Communication

Near Field Communication (NFC) embraces a set of communication protocols enabling devices to exchange data within a short distance of a few meters or even far below. It is based upon RFIDs. Today, NFC is commonly used for contactless payment systems, electronic keycard systems, and electronic identity documents, but may be also found in social networking for sharing small pieces of data, *e.g.,* contact information, photos, or files.

The technology is based on the ISO/IEC 18092:2004 standard revised by ISO/IEC 18092:2013 [47]. Devices are coupled and communicate over 13.56 MHz. The data rates supported range from 106 to 424 kbit/s. To exchange data between coupled devices three main requirements must be fulfilled: (a) The two devices need to be in range, (b) one device needs an Internet connectivity, and (c) the other device requires a corresponding application installed. Therefore, an NFC device can work in three modes [39]:

1. The "NFC card emulation"-Mode enables devices to act like smart-cards; the user can perform transactions, such as a public transport ticket's payment.

2. The "NFC reader/writer"-Mode allows to read information stored at specific tags; used in logistics or shops to collect detailed information on a product.

3. The "NFC peer-to-peer"-Mode is similar to an ad-hoc scenario allowing devices to exchange information with each other directly, such as via contactless chip-cards.

NFC transmitters can be active or passive [42], thus, the device can establish a connection on its own. Alternatively, the device has no power supply and cannot start a connection on its own. Thus, data may only flow in one direction, *e.g.,* from the tag to the smartphone.

Different organizations are responsible for different parts of the protocol stack depending on the signaling type used, *i.e.,* NFC-A, NFC-B, NFC-F, or P2P [54, 45]. Standardization organizations are responsible for physical characteristics and radio frequency specifications. The NFC Forum and vendor-specific organizations are only involved, if specific hardware and software is in place, which is highly influenced by applications.

12.3.8 Bluetooth (IEEE 802.15.1)

Bluetooth is a wireless communication standard for communications over short distances, *e.g.,* wireless headsets, which resulted in the standard IEEE 802.15.1 for PANs. It operates in the ISM band from 2.4 to 2.485 GHz, allowing for a data exchange between fixed and mobile devices as well as between two mobile devices within maximum range of 100 m. The radio technology deploys a frequency-hopping spread spectrum to enable sending of data in a robust manner. Bluetooth is a packet-based protocol, where a master and slaves form a piconet, which utilizes the same hopping sequence. While in general more than 200 devices can be part of a piconet, only 8 in total can be active due to the address space assigned. Parked devices can become active, if another device moves to park.

The hopping pattern within each piconet is determined by the master and the 1 MHz channel shared. In case a device wants to join the piconet and a slave position is free, it needs to synchronize with the hopping frequency used. The master coordinates the packet exchange with his clock ticking in 312.5 µs intervals. A slot is defined by two clock ticks resulting in 625 µs. The master always transmits in evenly numbered slots and receives in odd numbered slots, vice versa for all slaves. Depending on the number of devices participating in the communication, the throughput per device drops quickly due to the 1 MHz/s data rate. Thus, forming groups of piconets leads to scatternets, where overlapping communication ranges allow devices to participate in both piconets.

The Bluetooth protocol stack consists of a profile and core specification. The profile specification manages functions required to adapt the technology to legacy and new applications. The core specification includes all protocols required and supported from the PHY and MAC layer, including management functions. Those protocols include the following ones [60]:

- The radio element is responsible for the specification of the air interface: managing frequencies, modulation, and transmission power.

- The baseband element is responsible for the basic connection establishment, packet formats used, timing, and basic Quality-of-Service (QoS) parameters.

- The Link management protocol is responsible for setting up the link and the management, (*e.g.,* including security or parameter negotiation) between participating devices.
- The logical link control and adaptation protocol, the Logical link Control and Adaptation Protocol (L2CAP), handles the adaptation of higher layers to the base-band.
- The service discovery protocol checks the neighborhood of devices in close proximity and queries service characteristics of these.

On top of L2CAP other protocols are located dealing with the communication support, such as the cable replacement protocol and the telephony control protocol. The Host Controller Interface (HCI) is located between the base-band and the L2CAP and acts as a broker between hardware and software.

The *Bluetooth Low Energy (BTLE)* provides an energy saving version of Bluetooth [28]. It follows the master/slave architecture of piconets with a small modification: The slave sends advertising frames to discover the neighborhood on dedicated advertising channels. Thus, available masters scan those advertising channels, whether it has not yet reached the limit of the number of allowed slaves. If that has not been reached, the master was successful and the advertised slave becomes connected. In order to save slave's energy resources, the master defines individual cycles and scheduling sequences, which leads to the situation in which the slave is only awake if needed [18].

12.4 Cellular Networks (WAN)

Besides communication standards in use within the IoT context in the PAN and LAN area, WAN-related technical solutions exist, too. Since typically only resource-rich devices can make use of general public wireless access networks, such as cellular networks from the 1st to the 5th generation, with a clear exception of LTE in 4G and within 5G, only the major characteristics of cellular networks are discussed here. LTE for IoT will be refined in Section 12.5, since many IoT applications call for an operation over a longer distances at a higher cost.

12.4.1 General Architecture

Om general, a cellular network operates on the WAN basis and offers within "cells", each of which is equipped with a Base Station (BS) acting as a transceiver. Although the cell size varies between a few hundred meters up to 25 km, cells will overlap and, thus, communications for mobile devices, typically smartphones and tablets, need hand-overs between cells. Appropriate mobility support is embedded within the respective standards. As outlined in Figure 12.1, manifold communication standards for interconnecting IoT devices are in place, such as public wireless access networks in the generations 1G to 5G and less used privately operated networks, such as WiMax [60].

Cellular networks' architectures show a strong hierarchical approach, including within the BS a Base Transceiver Station (BTS) and a Base Station Controller (BSC), one or multiple Mobile Switching Centers (MSC), different location registers (home and visiting), and gateways to the Public Switched Telephone Network (PSTN). Those components inter-operate as follows [60]: Mobile devices call other devices by using E.164-based phone numbers, which are routed for remote receivers by the BS and the respective MSC to the serving MSC within the same cellular network or via the gateway to the PSTN. In case that phone number had been registered within the visiting register, a local MSC and its serving BS can route the call to the respective cell.

In order to communicate, all mobile devices have to hold a subscription to a public cellular network provided, who maintains user identification and relevant contractual data. In case this mobile device communicates within its home provider appropriate communication the local contract, including respective accounting and payment services, applies. Within a visiting cellular network communication only works is roaming agreements between the participating network providers exist and the mobile device's subscription allows for roaming services to be used.

While roaming support is required due to the mobility of devices, handovers between cells are based on signal monitoring. If the distance between a mobile device and the "old" BS grows beyond a certain threshold and if a "new" BS is in reach, four different hand-over scenarios can be distinguished: (a) and intra-cell hand-over within a single BTS' range, thus, onto a different frequency, (b) an inter-cell/intra-BSC hand-over between two different BTS, but one MSC, (c) an inter-BSC/intra-MSC hand-over between two different BSCs, but one MSC, and (d) an inter-MSC hand-over between different MSCs, which potentially can support inter-technology hand-overs. In case of a typically seamless hand-over the new connection to the new BS is established before the one to the old BS is cancelled, thus, the mobile device does not recognize the cell change at all.

The term "horizontal hand-over" had been introduced for similar technology in use, while a "vertical hand-over" happens between different communication technologies. The latter rise in importance for communications in an IoT context, since data or data flows from

sensor networks interconnected via a cellular network-enabled gateway provide long-distance access to these locally deployed networks.

12.4.2 System Generations

The set of standards for cellular networks has seen an almost 4 decades lasting development, including the generations 1G to 5G. Thus, Table 12.1 compares these cellular standards [14]. The development of the first generation 1G cellular networks supported approximately 2 kbit/s bandwidth based on purely analog communications. PSTNs had been interconnected with horizontal handovers only, while a dedicated communication channel (circuit) had to be established. This communication supports phone communications (voice), thus, circuit switching is based originally on FDMA (Frequency-Division Multiple Access).

Improvements in hardware capabilities, a full digitization of communications, and the rising number of mobile devices lead to the second generation 2G standard, including GSM, which delivered bandwidth between 14 to 64 kbit/s. Since the underlying core network remained unchanged as for 1G, horizontal handovers were supported only. All communications are based on FDMA, TDMA (Time-Division Multiple Access), or CDMA (Code Division Multiple Access). While for TDMA the same frequency of a channel is subdivided into time slots, each mobile device uses a negotiated time-slot, CDMA allows for several transmitters to send data simultaneously over a single communication channel (frequency) by applying orthogonal codes to each sender individually according to the spread spectrum model. Besides voice, 2.5G extended 2G by packet switching on top of existing circuits. Such software-only extensions into General Packet Radio Service (GPRS), High-speed Curcuit-switched Data Service (HSCDS), and Enhanced Data Rates for GSM Evolution (EDGE) in their basic forms.

Further technology developments resulted in the 3G standard, including extended GPRS and EDGE, which supports up to 2 Mbit/s per cell by applying Wideband-CDMA (W-CDMA) and interfacing for the first time directly to packet-based networks, such as an IP network. Besides high quality voice and video services, also data transmission was integrated. Thus, for data communications, the switching method "packet switching" required technical changes of the underlying cellular network architecture, except for the air interface. Thus, 3G packets consist of a header (used to route the packet) and a payload, including data extracted from the application or IoT devices interconnected. 3G technology still supports horizontal handovers only.

At the turn of the century, all-IP networks, fully packet-switched, broadband, and with a high speed (larger bandwidth up to 200 Mbit/s per cell), the convergence of WLAN/cellular and packet-based networks had been reached in a fully digital approach. The 4G standards include IMT2000 (International Mobile Telecommunications), UMTS (Universal Mobile Telecommunication System), HSDPA (High Speed Downlink Packet Access), LTE (Long Term Evolution), and LTE-A (Long Term Evolution Advanced). As a consequence the support of horizontal and vertical handovers became a reality and combined with the use of unified IP addresses the seamless convergence of PAN, LAN, MAN, and WAN networks was achieved. All switching is packet-based, and the Orthogonal Frequency-Division Multiple Access (OFDMA) had been deployed to provide robust and stable, high data rates. The service variety offered now access to any type of local network at the data level, thus, IoT-based communications can be integrated in 4G as long as an IoT gateway in service offers a 4G interface and interconnection. Since especially the LTE Category M (LTE Cat. M) and LTE Category N (LTE Cat. N) — also called Narrow Band (NB)-IoT — have been specified in 3rd Generation Partnership Project (3GPP)'s Release 13, they are discussed in special detail within Section 12.5.

Very recently, the 5th generation of cellular networks termed 5G has started operations, which means that up 20 Gbit/s bandwidth per cell are expected. Thus, massive capacity and massive connectivity, an increasingly diverse set of services and applications, and highly flexible and efficient use of available non-continuous frequency bands is at the doorstep. 5G is often nominated as the IoT enabler, since those billions of IoT devices already deployed and others to come can communicate now directly with the 5G network and, theoretically, do not necessarily need an IoT gateway anymore. However, this is only achieved, if power supply and device sizes are considered at right scales. Therefore, OFDMA-based communications via MIMO (Multiple-Input and Multiple-Output) antennas will still require for practical reasons a resource-rich IoT gateway device interfacing locally deployed IoT devices. Thus, the hierarchical structure of IoT-based networks, gateways, and public wireless access networks will remain, although the services being used directly and the bandwidth being available will enhance IoT-based use cases dramatically.

12.5 LTE Especially for IoT

As already introduced above, the 3GPP LTE standard offers two flagship techniques to transport data for IoT

Table 12.1: Comparison of Cellular Network Generations 1G to 5G based on [14]

	1G	**2G/2.5G**	**3G**	**4G**	**5G**
Development	since 1970	since 1980	since 1990	since 2000	since 2010
Operations	since 1982	since 1992/2000	since 2001	since 2004/2006/2009	since 2020
Standards	NMT, AMPS, TACS	2G: GSM, 2.5G: GPRS, HSCDS, EDGE	GPRS, EDGE, W-CDMA, CDMA-2000	UMTS, HSDPA, LTE and LTE-A	5G (MIMO)
Technology	Analog	Digital IP Access	Digital IP Access	Digital All IP	Digital Broadband All IP
Switching	Circuit	2G: Circuit 2.5G: Packet	Packet	All Packet	All Packet
Medium Access	FDMA	FDMA, TDMA, CDMA	FDMA, TDMA, CDMA	FDMA, TDMA, CDMA, OFDMA	FDMA, TDMA, CDMA, OFDMA
Bandwidth	2 kbit/s	14.4 ... 64 kbit/s	$<$ 2 Mbit/s	$<$ 200 Mbit/s	$>$ 1 Gbit/s
Core Network	PSTN	2G: PSTN 2.5G: Packet Network	Packet Network, Internet Access	Packet Network, Integrated Internet	All Internet
Hand-overs	Horizontal	Horizontal	Horizontal	Horizontal, Vertical	Horizontal, Vertical
Services	Voice	2G: Voice Short Messaging	Integrated 2.5G: Data	Integrated Voice and Data	All Data Voice and Data

applications, namely LTE Category M (LTE Cat. M) and LTE Category N (LTE Cat. N), which are also called Narrow Band (NB)-IoT and specified in 3GPP's Release 13. Two further approaches, the LTE Category 0 (LTE Cat. 0) and the Extended Coverage (EC)-GSM-IoT reduce the complexity of mobile devices, increase the sensitivity of the receiver allowing for lower Signal-to-Noise (SNR) regimes, decrease manufacturing costs of devices, and increase energy efficiency of network operations.

The main characteristics of LTE is that it is a cellular network (*cf.* Figure 12.10) working in the licensed radio spectrum range and is operated by the Mobile Network Operator (MNO). The Radio Access Network (RAN) in LTE relies on an evolved Node B (eNB), which is the central coordinator of the cell. The cell provides network coverage to Radio Frequency (RF)-enabled terminals, referred to as User Equipment (UE). UEs are mobile, so the mobility plays the key role in the design of cellular networks. A UE attached to an eNB can migrate to other cells via the hand-over mechanism, which in LTE is initiated by the serving eNB. The eNB uses the knowledge on the signal strength measurements of the neighboring cells reported by the UE to initiate a UE handover. LTE only supports a so called hard handover, in which a channel in the source cell is released and then the channel in the target cell is re-established [10].

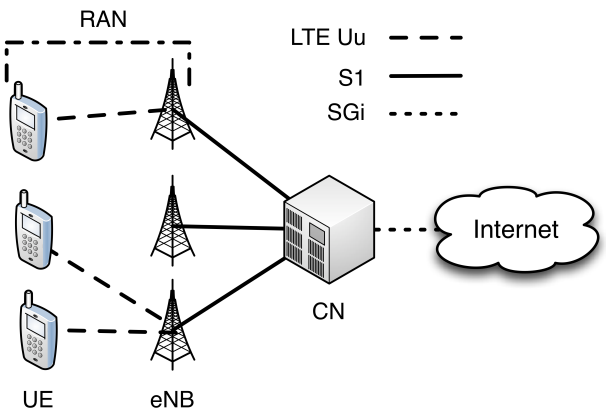


Figure 12.10: LTE Network Diagram.

12.5.1 Interfaces and Protocols

LTE specifies the radio interface (the so called LTE-Uu interface) to allow for a communication between an eNB and a UE using a vertical protocol stack with horizontally separated control and data planes (*cf.* Figure 12.11). The layers between the PHY Layer at the bottom and the Radio Resource Control (RRC) on the control plane (*cf.* Figure 12.11a) or the Packet Data Convergence Protocol (PDCP) on the data plane (*cf.* Figure 12.11b) at the top are referred to as the Access Stratum (AS). When a UE establishes an RRC connection to an eNB (on the control plane), the UE may communicate with the Non-Access Stratum (NAS) functionality exposed by the Core Network (CN). As an example, the LTE network attachment procedure, which activates radio and Evolved Packet System (EPS) bearers that, in turn, carry the Internet Protocol (IP) between the UE and the CN on the data-plane [59], is exposed through the CN NAS.

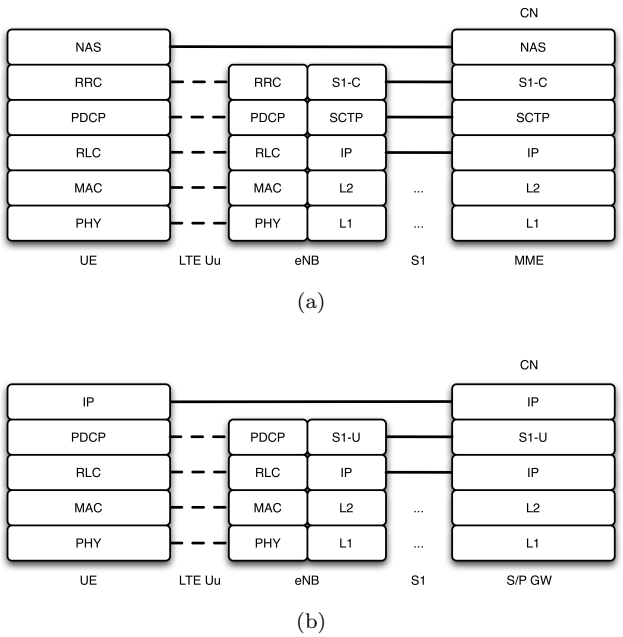


Figure 12.11: LTE Protocol Stack: a) Control Plane, b) User Plane

Radio Resource Control

The RRC protocol terminates the AS control plane on the eNB and provides the following functions: broadcast of AS/NAS system information, establishment, maintenance, and release of RRC connections between a UE and the eNB, radio and EPS bearer management, security handling, UE measurement reporting and configuration, handover, forwarding of NAS messages between the UE and the CN, and paging (initiate services for UEs being currently in the idle mode) [13]. Typically, protocols involved in the network operation operate in terms of Service Data Units (SDU) on the northbound and Protocol Data Units (PDU) on the southbound interface. The PDCP (Packet Data Convergence Protocol) [11] protocol, which is provided directly below the IP layer on the user plane (*i.e.,* the IP packet is the PDCP SDU) and the RRC layer on the control plane (*i.e.,* the RRC packet is also a PDCP SDU), is responsible for the compression of upper protocol layers as well as integrity protection and encryption [76].

Radio Link Control

The Radio Link Control (RLC) layer resides directly below the PDCP layer [11]. RLC operates in three modes, *i.e.,* Acknowledged Mode (AM), Unacknowledged Mode (UM), and Transparent Mode (TM). In AM, the SDU provided is segmented and acknowledged allowing for error correction through the Automatic Repeat reQuest (ARQ) mechanism as well as segmentation and reassembly, re-ordering, and duplicate detection. The UM only allows for segmentation with reordering and duplicate detection, while TM transparently passes PDCP SDUs (*i.e.,* no segmentation in this case) toward the MAC layer below, allowing for error detection with recovery.

The RLC defines logical channels focusing on the type of information transported through the underlying MAC layer. More specifically, different control channels are specified (*e.g.,* Broadcast Control Channel (BCCH), Common Control Channel (CCCH), Paging Control Channel (PCCH), and Dedicated Traffic Channel (DTCH) to transmit data (*cf.* Figure 12.12).

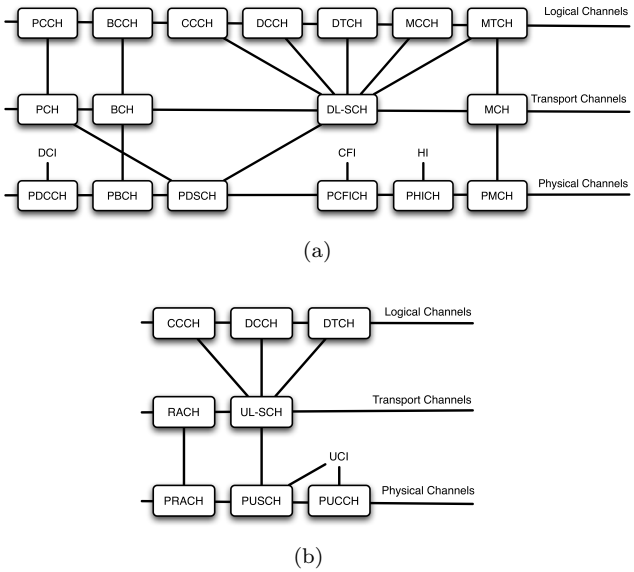


Figure 12.12: LTE Channel Structure: a) DL Channel Structure, b) UL Channel Structure

Medium Access Control

The MAC layer [76] receives RLC SDUs using logical channels and decides on how the SDU shall be transported to PHY through transport channels. There are only a few transport channels established between the MAC and PHY, *e.g.,* Broadcast Channel (BCH), Downlink Shared Channel (DL-SCH), Random Access Channel (RACH), or Uplink Shared Channel (UL-SCH). Typically, many logical channels working on the type of information basis, (*i.e.,* control or data) are sent over a single transport channel, therefore, MAC multiplexing and demultiplexing, respectively, is required in the Downlink (DL) and Uplink (UL) direction, respectively. The MAC layer also prioritizes logical channels among many UEs in the transport blocks. Moreover, the MAC is responsible for an Hybrid Automatic Repeat reQuest (HARQ), which is defined as a combination of Forward Error Correction (FEC) and ARQ mechanisms allowing

for a very fast retransmission of transport blocks within a time frame of smaller than 10 ms.

Typically, the information in the transport block is encoded using FEC, allowing the receiver to correct certain errors in the data stream received. Upon a successful reception of the information, the receiver issues an Acknowledgment (ACK) that notifies the transmitter about the successful reception, allowing the transmitter to continue with the subsequent transport blocks. However, when the information is received incorrectly, the receiver issues a Negative Acknowledgment (NACK), which triggers a retransmission of lost data at the transmitter. Normally, the majority of transmission (TX) errors is corrected by the HARQ mechanism.

Finally, the MAC layer is also involved in control operations, such as (a) Discontinuous Reception (DRX), in which the UE changes its status from RRC_CONNECTED (*i.e.,* with connected Signaling (SRB) and Data (DRB) Radio Bearers) to RRC_IDLE, in which radio bearers are disconnected and the node should only monitor the PCCH for upcoming Mobile Terminated (MT) requests to save power, (b) alignment of the UL Timing Advance (TA) on the connected UE, (c) power head-room reporting, in which UEs notify the eNB about the remaining power room on the UL to influence on scheduling, (d) scheduling of UE UL transmissions, and (e) Random Access (RA) providing resources to UEs without allocated resources.

Physical

The LTE PHY [52] uses a hybrid access scheme consisting of Orthogonal Frequency-Division Multiple Access (OFDMA) on the UL and Single-Carrier Frequency-Division Multiple Access (SC-FDMA). Such an asymmetric access technique solves the peak-to-average power ratio problem of OFDMA. In Orthogonal Frequency-Division Multiplexing OFDM, the Fast Fourier Transform (FFT) may produce a high peak power to average power value. OFDM, has to be, therefore, avoided in transmitters on client terminals, as it may only be used on grid-powered eNBs. SC-FDMA seems to be a good solution for end-terminals for mitigating the problem of power peaks.

The LTE PHY features a high spectrum flexibility, while the frequency spectrum is scheduled dynamically to UEs through Physical Resource Blocks (PRB). Every PRB consists out of 180 kHz blocks (*cf.* Figure 12.13), *i.e.,* 12 subcarriers, and lasts 1 ms, while every subcarrier spans a 15 kHz spectrum range (*i.e.,* 15 kHz subcarrier spacing) [26]. LTE supports two fundamental modes of operations of PHY, *i.e.,* LTE Frequency Division Duplex (LTE-FDD) and LTE Time Division Duplex (LTE-TDD). LTE-FDD operates in paired frequency ranges, meaning two disjoint spectrum ranges for UL and DL. LTE-TDD uses an unpaired channel. Therefore, UL and DL are carried out in a single channel, where UL is separated from DL in time. LTE-FDD is by nature full-duplex, however, when a UE cannot transmit and receive at the same time, the LTE-FDD-half duplex can be used. LTE-TDD is, in turn, by nature a half-duplex mode of operation. Full-duplex LTE-FDD requires a duplexer to separate UL and DL frequencies on the UE to avoid the reception port (RX) saturation through the TX port working in parallel. Half-duplex LTE-FDD and LTE-TDD do not, in turn, require duplexers in the radio chain, since LTE TX and RX do not operate at the same time.

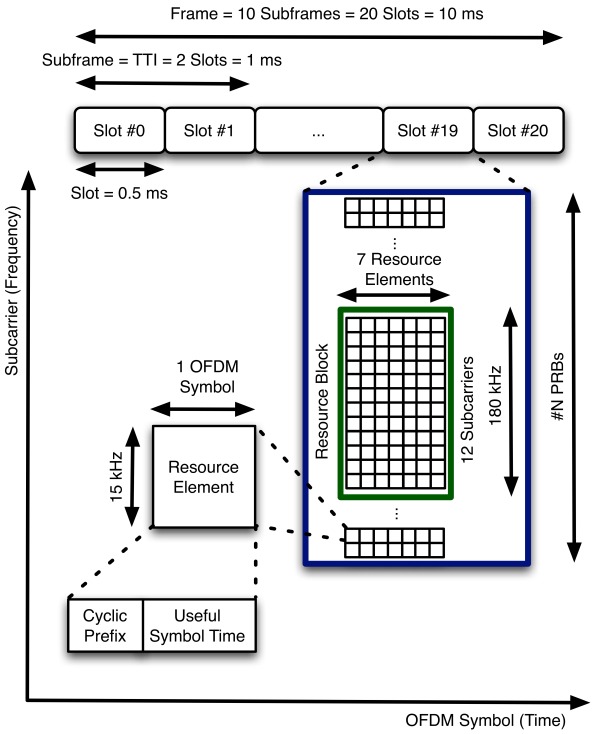


Figure 12.13: LTE Frame Diagram

Two logical frame structures are specified in PHY. Type 1 specifies the communication in LTE-FDD, while Type 2 is used in LTE-TDD. The frame defines a resource grid of PRBs, responsible for carrying the control and data plane data stream as well as providing synchronization and random access for end terminals. The frame, lasting 10 ms, consists out of 10 subframes (SFs) of 1 ms each, which contain 2 time slots of 0.5 ms. Every slot is composed out of 7 OFDM symbols, where each symbol begins with the Cyclic Prefix (CP) that protects symbols against Inter Symbol Interference (ISI) through a guard period between symbols in the time domain. At the smallest scale, the PHY consists of one OFDM sub-

carrier during one OFDM symbol interval.

The available channel bandwidths are 1.4, 3, 5, 10, 15, and 20 MHz, which allocate a parallel set of 6, 15, 25, 50, 75, and 100 PRBs, respectively [15]. There are two levels of guard band overheads protecting channels, *i.e.,* 23% for the 1.4 MHz channels and 10% for other bandwidths (3, 5, 10, and 20 MHz). These guard bands are used to protect the channel against unwanted emissions in neighboring frequency ranges. Furthermore, in LTE-TDD, a Gap Period (GP) between the DL and UL transmissions is introduced through a Special SubFrame (SSF) of 1 ms to give UEs time to change from the DL (RX) to the UL (TX) operation. The GP can be considered a waste of spectrum, since no transmission on an eNB or UE is carried out during this time interval anyway.

LTE Transmission Intervals

All the transmission intervals in the time domain are expressed in terms of the basic time unit T_S equaling to 1/30720000 s (*i.e.,* the sample time). The useful symbol duration, which carries out the transmitted information, is equal to $2048 \times T_S$, which is roughly 67 µs. The regular CP is equal to $160 \times T_S$ (i.e., 5.2 µs) for the first symbol and $144 \times T_S$ (i.e., 4.7 µs) for the remaining six symbols in the time slot, which sums up to a total time slot duration of $15360 \times T_S$ (i.e., 0.5 ms). The SF duration is established at $30720 \times T_S$ (i.e., 1 ms) as every SF is composed of two time slots lasting $15360 \times T_S$ each. Finally, the frame duration is equal to $307200 \times T_S$ (i.e., 10 ms), while every frame is composed of 10 SFs [52].

12.5.2 LTE (3GPP Release 8)

3GPP Release 8 standardizes LTE with five UE categories (*i.e.,* Cat. 1, . . . , Cat. 5). Release 8 uses varying modulation and coding rates as well as spatial multiplexing provided through Multiple-Input Multiple-Output (MIMO). The data rate experienced by upper protocol layers on an end terminal (*i.e.,* termed goodput) depends on a so called Modulation and Coding Scheme (MCS). MCS varies between 0 and 27 and indicates the modulation and coding rate. Three modulation techniques were initially introduced, *i.e.,* Quadrature Phase-Shift Keying (QPSK), which is mathematically equivalent to 4-Quadrature Amplitude Modulation (QAM), 16-QAM, and 64-QAM of efficiency $Q_m = 2$, 4, and 6 bits per symbol, respectively, where the modulation efficiency is understood as the number of bits encoded in one symbol. While the modulation influences the number of bits sent in one symbol, the code rate defines the amount of redundant information inserted into the data stream for the FEC. Finally, the spatial multiplexing configures the number of so called MIMO layers, *i.e.,* independent data streams sent from multiple antennas on the transmitter towards multiple antennas on the receiver. 1×1 MIMO materialized by one antenna on the transmitter and one antenna on the receiver is called Single Input Single Output (SISO) and allows for one MIMO layer.

In the SISO mode, the available UL throughput of LTE in Release 8 using the EU of Cat. 5 is established at 100 Mbit/s, when the maximal channel width, modulation efficiency, and FEC code rate (*i.e.,* the fraction of useful or non-redundant information in the data stream) are equal to 20 MHz, 64-QAM, and 1, respectively. Conceptually explained within the frequency domain, a 20 MHz channel carries 100 parallel PRBs and every PRB consists out of 12 independent subcarriers, resulting in 1200 parallel subcarriers. In the time domain, a PRB lasts 1 ms and consists out of two time slots. Every time slot holds 7 OFDM symbols, thus, resulting in 14 OFDM symbols. When the 64-QAM modulation is used, $Q_m = 6$ bit might be carried out by one OFDM symbol. Thus 100,800 bit (*i.e.,* $1200 \times 14 \times 6$ bit) may be transported using all 100 parallel PRBs in the frequency domain within 1 ms in the time domain, thus, resulting in 100.8 Mbit/s. LTE specifications (*i.e.,* different releases) often present the system capacity using the number of bits that may be inserted into the LTE frame within a Transmission Time Interval (TTI) of 1 ms.

MIMO systems achieve a much better performance in comparison to SISO systems, since the increased throughput in the SISO mode requires modulations of higher efficiencies and high code rate, which typically imposes a higher SNR and a lower link budget. MIMO comes, however, at the price of independent RX/TX radio chains implemented on the communicating device. Release 8 supports up to 300 Mbit/s DL and 75 Mbit/s UL using its highest UE category through the introduction of up to 4 parallel data streams using 4×4 MIMO.

12.5.3 LTE Advanced (3GPP Release 10)

3GPP Release 10 standardizes LTE Advanced (LTE-A) exploring MIMO and carrier aggregation (both continuous and non-continuous channel aggregation techniques are taken into account combining up to 5 independent channels) to increase throughout. Three new UE categories were introduced (*i.e.,* Cat. 6, . . . , Cat. 8). LTE Cat. 8 equipment is theoretically able to reach the momentary DL of 3 Gbit/s and UL of 1.5 Gbit/s respectively by using 64-QAM, 8 parallel data streams

achieved through 8×8 MIMO, and continuous channel aggregation of five 20 MHz bandwidths in LTE-TDD.

3GPP Release 11 extends LTE-A with the specification of three UE classes (*i.e.,* Cat. 9, ..., Cat. 12) using 256-QAM, 2 and 4-layered MIMO (*i.e.,* 2 or 4 independent data streams), while Release 12 improves the throughput of LTE-A in new equipment classes (*i.e.,* Cat. 13, ..., Cat. 16) due to the combination of 8 MIMO layers with the 256-QAM modulation providing 3.9 Gbit/s in an LTE UE of Cat. 14.

LTE Cat. 0 is the first UE category targeting IoT devices explicitly as described in 3GPP release 12 [10] standardizing LTE-A Pro. It is based on the previously specified hybrid PHY with OFDMA-based UL and SC-FDMA-based UL with certain modifications. The maximum output power remains at the Power Amplifier level of Class 3, *i.e.,* 23 dBm. The number of antennas is fixed to one (SISO), therefore, the spatial multiplexing (*i.e.,* MIMO) is not supported. LTE Cat. 0 does not support highly efficient modulation techniques, such as 256-QAM, on the DL and 64-QAM UL leaving the device with QPSK, 16-QAM, 64-QAM (DL) as well as QPSK and 16-QAM (UL). Furthermore, LTE Cat. 0 supports 1.4, ..., 20 MHz channels, however, limits the number of bits per TTI of the UE to 1000 bit, which ultimately fixes the UE DL/UL upper transmission capacity at 1 Mbit/s. The device may operate in the full duplex mode and two half duplex modes of type A and and B.

Typically, in the regular LTE-FDD half-duplex mode A, when a UE is scheduled to transmit in UL SF n, no transmission is scheduled toward this UE in the UL SF n either. Furthermore, a special Guard Period (GP) spanning a fraction of the previous DL SF $n-1$ is introduced to allow for safe switching from RX to TX on the UE without loosing any data on the DL. In the newly introduced LTE-FDD half-duplex mode B, the GP period was enlarged. When a UE is scheduled to transmit in UL SF n, no DL transmission toward this UE is allowed in SFs $n-1$, n, and $n+1$ to further relax the speed of RX/TX switching.

Typically, when a device connects to an eNB, it has to comply with DRX by monitoring the paging channel for incoming Mobile Terminated (MT) transmissions. A regular UE paging cycle is 128 frames, meaning 1.28 s (*i.e.,* 1280 ms as the frame duration is 10 ms), in which the device has to wake up and listen to the PCCH for MT transmissions. This might be too power-hungry in the case of battery-powered IoT devices. Therefore, a Power Saving Mode (PSM) was introduced (*cf.* Figure 12.14), which allows the network node to negotiate an extensive Tracking Area Update (TAU)/Routing Area Update (RAU) timer (T3412) and Active Mode Timer (T3324). The Mobile Originated TAU message

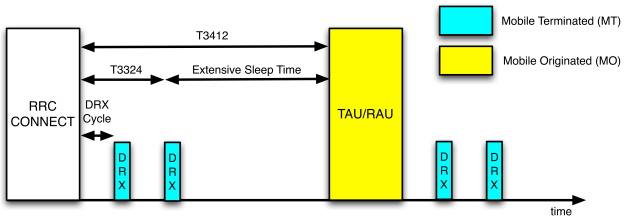


Figure 12.14: LTE Power Saving Mode (PSM)

is used to notify the network, about the current UE location in the idle mode (*e.g.,* for MT transmissions). Typically, the TAU message is sent upon the location change or timer expiration (*i.e.,* T3412). Additionally, the Active Mode Timer (*i.e.,* T3324) defines for how long the timer is set since the RRC_CONNECT or last TAU was received. The UE shall monitor PCCH with a regular paging cycle specified by the network. When T3324 expires, the UE may go to an extensive sleep mode, not issuing or accepting, respectively, any MO or MT message, respectively. Therefore, the time period of T3412−T3324 is referred to as a "hibernation period", after which the UE wakes up, sends a MO TAU message, and repeats the PSM cycle again (*e.g.,* being in the RRC_IDLE mode) [48].

12.5.4 LTE Advanced Pro

LTE Advanced Pro offers two equipment categories especially for IoT purposes, *i.e.,* LTE Cat. M and LTE Cat. N, which are specified as 3GPP Release 13.

LTE Category M

LTE Cat. M1 [46] specified in Release 13 is based on the work performed in Release 12. The UE peak data data rate is again limited, as in the case of LTE Cat. 0, through the number of bits per TTI and per UE to 1000 bit, which fixes the UE DL/UL upper transmission capacity at 1 Mbit/s. It provides mobility through a handover operation, *i.e.,* UE measurement reporting, RRC connection release, and RRC re-establishment. Furthermore, voice communication is supported. Many simplifications of the physical layer were performed. The bandwidth is reduced to 1.4 MHz (*i.e.,* 6 PRBs) and two Power Amplifier (PA) classes were introduced, *i.e.,* Class 5 with 20 dBm and Class 3 with 23 dBm. Two Coverage Enhancement (CE) modes were added, in which the mandatory CE Mode A and optional CE mode B (*i.e.,* deep coverage) support up to 32 and 2048 repetitions, respectively. Physical channel repetition means that the same message is sent many times with-

out waiting for the HARQ confirmation at the distinct TTI level.

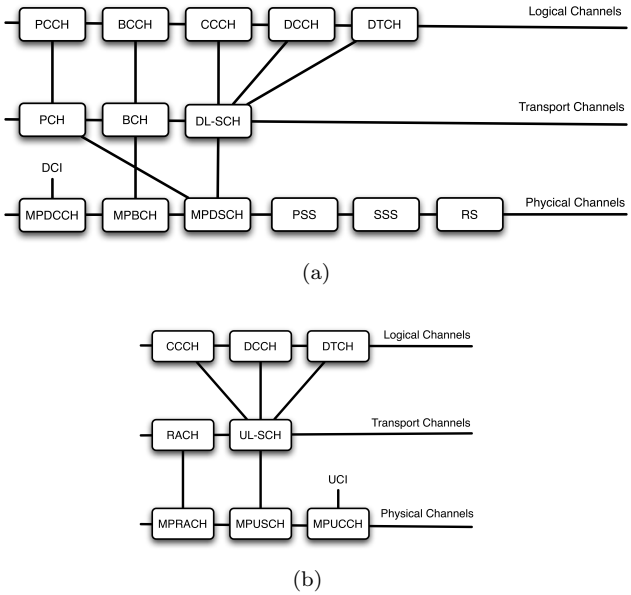


Figure 12.15: LTE-M Channel Structure: a) DL Channel Structure, b) UL Channel Structure

In the PHY layer, the Primary Synchronization Signal (PSS), the Secondary Synchronization Signal (SSS), and the Reference Signal (RS) known from the regular LTE standard provide the means to synchronize a UE with the cell, thus, they are fully re-used (*cf.* Figure 12.15). The DL specifies the following PHY channels: Machine Type Communication (MTC) Physical Downlink Control Channel (MPDCCH), MTC Physical Broadcast Channel (MPBCH), and Physical Downlink Shared Channel (MPDSCH). Please not that there is no Physical Control Format Indicator Channel (PCFICH) or Physical HybridARQ Indicator Channel (PHICH) as known from regular LTE. The reasoning behind this concept is the following. First, the MPDCCH is of fixed size, *i.e.,* 2, 4, or 6 PRBs, which also carry HARQ feedback, *i.e.,* Downlink Control Information (DCI). Therefore, the PDCCH size adjustment is not needed. Second, the HARQ process on the UL is asynchronous, *i.e.,* scheduled, therefore, the PHICH channel is not necessary. In regular LTE, however, HARQ is a synchronous operation always completing within 8 ms through its special-purpose PHICH channel. The number of HARQ processes (*i.e.,* the number of outstanding, but not yet confirmed blocks) is 8 and 1 in CE Mode A and CE Mode B, respectively [40].

Furthermore, the MPDSCH is the DL shared channel to send unicast data toward the UE. On the UL, MTC Physical Random Access Channel (MPRACH), MTC Physical Uplink Shared Channel (MPUSCH), and MTC Physical Uplink Control Channel (MPUCCH) exist. The MPRACH is used to request a connection with an eNB or request UL resources, if the MPUCCH channel is not yet provided with the UE. MPUCCH is of fixed 1 PRB size. It is used to transport scheduling requests, provide HARQ feedback, *i.e.,* Uplink Control Information (UCI), or to send the Channel Quality Information (CQI). Finally, MPUSCH is used to send unicast traffic of 1-6 PRBs in CE mode A and 1-2 PRBs in CE mode B. LTE Cat. M only supports QPSK and 16-QAM modulations on the MPUSCH/MPDSCH channels, while MCS varies between 1 and 15. The Maximum Coupling Loss (MCL) shall be significantly improved through repetitions reaching 155.7 dB, *i.e.,* 15 dB higher in comparison to Release 12 systems [46].

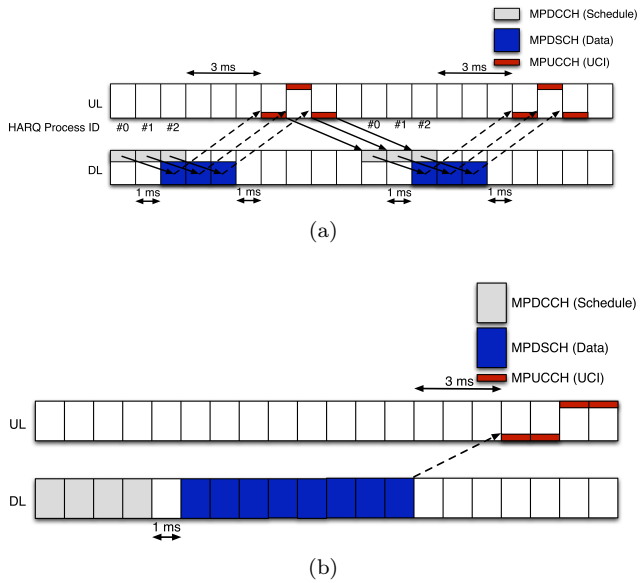


Figure 12.16: Example LTE-M Transmissions: a) Regular DL Transmission, b) DL Transmission with Repetition and Frequency Hopping

Figure 12.16 displays example DL transmissions in LTE-M. In Figure 12.16a 6 blocks (of 4 PRBs) are sent over the MPDSCH channel. Every distinct MPDSCH block is scheduled first using a corresponding MPDCCH channel (of 2 PRBs) and later acknowledged (*i.e.,* ACK) through the MPUCCH channel (of 1 PRB). The eNB uses 3 HARQ process of IDs #0,...,#3. There are 1 ms distances between: (a) the corresponding MPDCCH and MPDSCH messages, (b) DL and UL, and (c) UL and DL. The spacing between corresponding MPDSCH and MPUCCH (*i.e.,* UCI) channels remains equal to 3 ms as in regular LTE, however, the HARQ delay grows to 10 ms (*i.e.,* +2 ms in comparison to the regular LTE) due to the MPDCCH/MPDSCH and and DL/UL separation of 1 ms (*i.e.,* relaxed DL/UL switching on the UE). Additionally, Figure 12.16b dis-

plays an example transmission of 1 MPDSCH channel (of 6 PRBs) repeated 8 times. The block is scheduled through 1 MPDCCH channel (of 6 PRBs) repeated 4 times and acknowledged by 1 MPUCCH channel (of 1 PRB) repeated 4 times using a frequency hopping technique [40].

The battery power is extended by the PSM mechanism as specified already in Release 12 or by a newly specified Extended DRX (eDRX) mechanism (*cf.* Figure 12.17). The eDRX mechanism does not work on the TAU expiration basis meaning that the TAU MO does not have to be sent. Instead, the UE just notifies the eNB on the number of DRX cycles to be skipped on a periodic basis. First, the UE listens to the paging channel (*e.g.,* using the regular paging cycle of 1,280 ms) during the Paging Time Window (PTW) and, second, enters an extended sleep for a specific period of time defined in the number of hyperframes (HFN) to be skipped. A hyperframe consists of 1024 frames, *i.e.,* 0,. . . , 1023, and lasts for 10.24 s. When the extended sleep expires, the device wakes up again and repeats the eDRX procedure all over again [48].

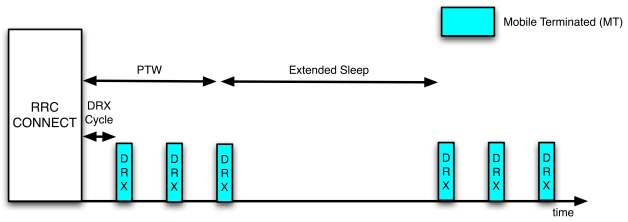


Figure 12.17: LTE Extended Discontinuous Reception

LTE Category N

The LTE Cat. N (also referred to as NB-IoT) [48] is a new PHY layer established in 3GPP Release 13 using 200 kHz channels (*i.e.,* one PRB of 180 kHz with 10 kHz guard bands on both channel edges). The peak data data rate of NB-IoT is 16 kbit/s on the UL and 26 kbit/s on the DL, while the bandwidth is only 200 kHz. The link budget is at 164 dB, while only Binary Phase Shift Keying (BPSK) and QPSK modulations with up to 2048 repetitions on the DL and 128 repetitions on the UL are used. In contrast to LTE Cat. M, LTE Cat. N does not support mobility (*i.e.,* handovers) or voice.

Three different deployment modes are specified: (1) stand alone operation used within the currently used GSM frequency plan, while the GSM channel bandwidth is at 200 kHz, (2) guard band operation utilizing unused resource blocks of other channels within an LTE carrier guard-band, and (3) in-band operation utilizing already allocated resource blocks within a given LTE carrier.

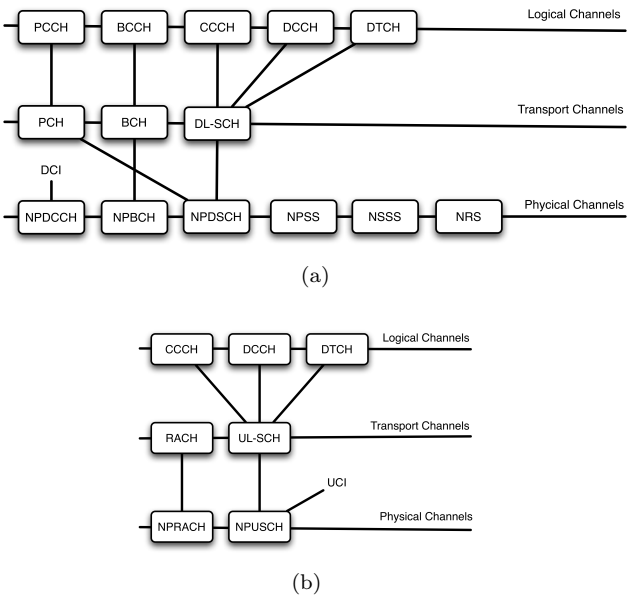


Figure 12.18: LTE-N Channel Structure: a) UL Channel Structure, b) UL Channel Structure

The PHY operation in the NB spectrum resembles the regular LTE operation. In LTE Cat. N DL PHY, OFDMA is used as an access technique. In time domain, a radio frame comprises of 10 SFs. Each SF spans 1 ms and contains 2 slots, and each slot contains 7 OFDM symbols. Within each Radio Frame, the SFs are labelled from 0 to 9 and the slots from 0 to 19. The frames in a hyper frame are numbered with a System Frame Number (SFN), which ranges from 0 to 1023. These hyperframes are also numbered with values between 0 and 1023, therefore, the numbering reflects the regular LTE system. In the UL, SC-FDMA is applied with 3.75 kHz or 15 kHz subcarrier spacing in the frequency domain. In the time domain, with the subcarrier spacing of 15 kHz (regular LTE), each slot has a duration of 0.5 ms, the number of subcarriers is 12. With the subcarrier spacing of 3.75 kHz, each slot has a duration of 2 ms, while the number of subcarriers is 48.

LTE Cat. N defined new channels at the PHY layer on the DL meaning Narrowband Primary Synchronization Signal (NPSS), Narrowband Secondary Synchronization Signal (NSSS), Narrowband Physical Broadcast Channel (NPBCH), Narrowband Reference Signal (NRS), Narrowband Physical Downlink Control Channel (NPDCCH), and Narrowband Physical Downlink Shared Channel (NPDSCH) (*cf.* Figure 12.18).

For the stand-alone and guard-band deployments, no LTE resource needs to be protected, therefore, DL NPDCCH, NPDSCH, or NRS may utilize all resource elements in one PRB pair (defined as 12 subcarriers over one SF). For in-band deployment NPDCCH,

NPDSCH, or NRS cannot be mapped to resource elements taken by LTE Cell-Specific Reference Symbols (CRS) and LTE Physical Downlink Control Channel (PDCCH) to comply with the regular LTE PHY format. On the UL, Narrowband Physical Random Access Channel (NPRACH), Narrowband Physical Uplink Shared Channel (NPUSCH), Demodulation Reference Signal (DMRS) are specified. It is worth noting at this point that the LTE Cat. N physical N-channels, *e.g.,* NPRACH, roughly correspond to LTE Cat. M M-physical channel functions, *e.g.,* MPRACH, however, they are specified on a much lower spectrum range allocated at the RE basis [61].

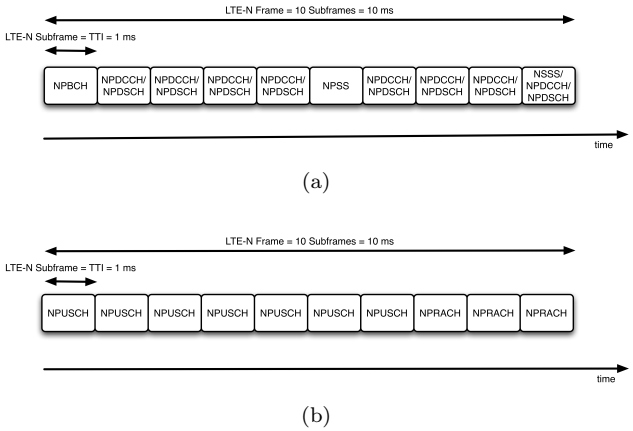


Figure 12.19: LTE-N Frame Structure: a) DL Frame Structure, b) UL Frame Structure

The DL frame shows the following organization: NPBCH commences the frame in SF 0, SF 1-4 carry NPDSCH or NPDCCH, the Primary Cell Reference Signal is located in SF 5, cells 6-8 may again hold the NPDSCH or NPDCCH, and SF 9 may posses the Secondary Reference Signal, NPDSCH, or NPDCCH. The UL frame is composed out of NPUSCH in SF 0-6 and NPRACH frames in SF 7-9 [43], respectively (*cf.* Figure 12.19). The UL access is requested through the NPRACH channel, which is implemented through the six tone frequency hopping scheme on the RE basis.

12.6 Summary and Conclusions

As of today a wide range of Internet-of-Things (IoT) devices — "the things" — is capable of collecting, processing, and transmitting data to servers and applications. While in the meantime the number of these devices reached the billions, their heterogeneity is very large, too, ranging from dust-like devices — belonging to the constrained devices' category — to resource-rich devices. In the same dimension the various types of protocols available enable communications, either between IoT devices or via an IoT gateway to the outside world.

IoT involves a huge range of players from industry, government, application developers, and private activities. Thus, use cases scale from a single constrained device up to massive cross-country and cross-platform deployments of heterogeneous, embedded IoT devices connecting to the outside world in terms of dedicated control centers or just the Cloud. While the specific communication demands range from low-level data rates to real-time requirements, many legacy and newly emerging IoT communication protocols allow IoT devices and servers to interact in tightly, loosely interconnected as well as secured ways. This did lead to dozens of competing alliances and coalitions of stakeholders to pave a path of unifying the highly fractured IoT domain.

12.6.1 Chapter Digest

This chapter provided an overview specifically on network communication technologies and their related protocols used in the IoT environment, while the focus was laid briefly in a basic introduction on the infrastructure perspective with Ethernet and IP and in-depth on IoT data communications and transport protocols.

Several technologies were presented for the PAN, LAN, and WAN coverage, while the focus was laid on the infrastructure perspective and IoT data communications and transport protocols. While for the former had been recalled briefly by Ethernet and IPv4 details, for the latter wireless PAN and LAN protocols include IEEE 802.11 (WiFi), IEEE 802.15.4 with the ZigBee, 6LoWPAN, BLIP, and Sigfox protocol stacks, LoRa, DASH7, RFID including Z-Wave, NFC, and Bluetooth as IEEE 802.15.4.

Additionally, WAN protocols surveyed include the general architecture of public wireless access networks in their generations 1G to 5G, and more specifically the 4G cellular LTE technology for IoT concentrating on LTE Cat. 0 (3GPP Release 8), LTE Cat. 8 (3GPP Release 10) as of LTE Advanced, and LTE Cat. M, LTE Cat. N, and LTE Cat. M1 (3GPP Release 13) as of LTE Advanced Pro.

12.6.2 Concluding Observations

The major dimensions to consider upon selecting one of these network communication technologies for a given IoT system include a larger list: (a) device type(s) to be supported and constrained network topology required, (b) licensed or free spectrum to be used, (c) geographical distance or range to be covered, (d) bandwidth offered (point-to-point versus shared), (e) energy demands, (f) open or proprietary specification or standard, (g) security measures available on the IoT device level, the

protocol level, or the application level, while the role of the IoT gateway has to be determined first, and (h) the costs involved in regular, frequent, infrequent communications and related flat charges for subscriptions.

Overall, data transfer within the IoT domain will successfully be accepted by the public only, if communications between interconnected IoT devices in use and the outside world is secured, which is especially highly important in case of privacy-related applications of the health domain or home automation. A much wider security analysis of those standards as selected above can reveal in the future further in-depth information about where and at which level to find security provisioning in IoT (such as performed exemplarily within [63]) and for which protocols further security demands may have to be integrated.

It must be emphasized that especially cellular networks as IoT communication technologies in the 4th and 5th generation will play a key role to build an active part in IoT scenarios. Besides classic devices for cellular networks, such as smartphone, tablets, and navigation devices, the set of constrained devices in the range of sensors, small actuators, and controllers, will help to integrate locally distributed information in such a way that regional or more global data collections (hopefully being fully compliant with privacy protection guidelines and regulations) can optimize the operation of, *e.g.,* manufacturing processes, energy harvesting or production systems, or elderly living homes. The path to travel further is still long and network communication technologies provide the underlying basis for all of these.

Acknowledgements

This paper was supported partially by *(a)* the University of Zürich UZH, Switzerland and *(b)* the European Union's Horizon 2020 Research and Innovation Program under Grant Agreement No. 830927, the CONCORDIA project.

12.7 Bibliography

[1] "AN1200.22 LoRa Modulation Basics," http://wiki.lahoud.fr/lib/exe/fetch.php?media=an1200.22.pdf, last access: April 20, 2020.

[2] "Arduino-based Library for Dragino Lora Shield v1.4 https://github.com/arduino-org/arduinolibrary-lora-node-shield." last access: April 20, 2020.

[3] "Arduino Products, https://www.arduino.cc/en/Main/Products," last access: April 20, 2020.

[4] "LoRa signals from a low orbit satellite," https://twitter.com/telkamp/status/956900631985475586?lang=en, last access: April 20, 2020.

[5] "SX1272/3/6/7/8: LoRa Modem, Designer's Guide," https://www.rs-online.com/designspark/rel-assets/ds-assets/uploads/knowledge-items/application-notes-for-the-internet-of-things/LoRa%20Design%20Guide.pdf, last access: April 20, 2020.

[6] "IEEE 802.11 Wirless Local Area Networks," http://www.ieee802.org/11/, November 2017, last access: April 20, 2020.

[7] "IEEE 802.3 Ethernet Working Group," http://www.ieee802.org/3/, October 2017, last access: April 20, 2020.

[8] "International Organization for Standardization," https://www.iso.org/standards.html, November 2017, last access: April 20, 2020.

[9] "The Things Network," https://www.thethingsnetwork.org/, last access: April 20, 2020.

[10] 3GPP, "TS 36.306: Evolved Universal Terrestrial Radio Access (E-UTRA); User Equipment (UE) radio access capabilities (Release 12)."

[11] 3GPP, "Evolved Universal Terrestrial Radio Access (E-UTRA); Packet Data Convergence Protocol (PDCP) specification (Release 13)," June 2017.

[12] N. Abramson, "THE ALOHA SYSTEM: Another Alternative for Computer Communications," in *Proceedings of the November 17-19, 1970, Fall Joint Computer Conference*, ser. AFIPS '70 (Fall). New York, NY, USA: Association for Computing Machinery, 1970, p. 281–285. [Online]. Available: https://doi.org/10.1145/1478462.1478502

[13] S. Ahmadi, "Chapter 5 - Radio Resource Control Functions," in *LTE-Advanced*, S. Ahmadi, Ed. Academic Press, 2014, pp. 227 – 287. [Online]. Available: http://www.sciencedirect.com/science/article/pii/B9780124051621000058

[14] S. Akhtar and M. Pagani, "2G-5G Networks: Evolution of Technologies, Standards, and Deployment," in *Encyclopedia of Multimedia Technology and Networking*. Hershey, PA, USA: IGI Global, 2009, vol. 2, pp. 522–532.

[15] I. Alyafawi, E. Schiller, T. Braun, D. Dimitrova, A. Gomes, and N. Nikaein, "Critical Issues of Centralized and Cloudified LTE-FDD Radio Access Networks," in *2015 IEEE International Conference on Communications (ICC)*, June 2015, pp. 5523–5528.

[16] F. Baker, "Requirements for IP Version 4 Routers," RFC 2460 (Internet Standard), RFC Editor, Jun. 1995. [Online]. Available: https://www.rfc-editor.org/rfc/rfc1812.txt

[17] Berkeley WEBS, "Project Page for blip, the Berkeley IP implementation for low-power networks," http://tinyurl.com/bliptutorial, October 2011, last access: April 20, 2020. [Online]. Available: http://tinyurl.com/bliptutorial

[18] C. Schmitt, "Trust & Security in IoT: Monitoring with Constrained Devices," Habilitation, Universität Zürich, Zürich, Switzerland, September 2019.

[19] V. Cerf, Y. Dalal, and C. Sunshine, "Specification of Internet Transmission Control Program," RFC 675 (Historic), RFC Editor, Fremont, CA, USA, pp. 1–70, Dec. 1974, obsoleted by RFC 7805. [Online]. Available: https://www.rfc-editor.org/rfc/rfc675.txt

[20] S. Chakrabarti, G. Montenegro, R. Droms, and J. Woodyatt, "IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) ESC Dispatch Code Points and Guidelines," RFC 8066 (Proposed Standard), RFC Editor, Fremont, CA, USA, pp. 1–9, Feb. 2017. [Online]. Available: https://www.rfc-editor.org/rfc/rfc8066.txt

[21] Chipcon AS SmartRF, "CC2420 Preliminary Datasheet (rev 1.2)," September 2004, last access: April 20, 2020. [Online]. Available: http://inst.eecs.berkeley.edu/~cs150/Documents/CC2420.pdf

[22] CISCO, "Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2017–2022," CISCO, San Jose, CA, USA, Tech. Rep. C11-738429-01, February 2019.

[23] S. Dawson-Haggerty, A. Tavakoli, and D. Culler, "Hydro: A Hybrid Routing Protocol for Low-Power and Lossy Networks," in *1st IEEE International Conference on Smart Grid Communications*, ser. SmartGridComm. New York, NY, USA: IEEE, October 2010, pp. 268–273.

[24] DIGI, "XBee®/XBee-PRO S2C ZigBee - RF Module User Guide," Digi International Inc., Minnetonka, MN, USA, Tech. Rep., September 2017.

[25] J. Donaldson, "RFID Started The Internet of Things Movement... Now It's Set to Lead It," https://www.mojix.com/rfid-internet-of-things-movement/, October 11 2016, last access: April 20, 2020.

[26] M. Elsaadany, A. Ali, and W. Hamouda, "Cellular LTE-A Technologies for the Future Internet-of-Things: Physical Layer Features and Challenges," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 4, pp. 2544–2572, 2017.

[27] V. Fuller and T. Li, "Classless Inter-domain Routing (CIDR): The Internet Address Assignment and Aggregation Plan," RFC 4632 (Best Current Practice), RFC Editor, Fremont, CA, USA, pp. 1–27, Aug. 2006. [Online]. Available: https://www.rfc-editor.org/rfc/rfc4632.txt

[28] C. Gomez, J. Oller, and J. Paradells, "Overview and Evaluation of Bluetooth Low Energy: An Emerging Low-power Wireless Technology," *IEEE Communications Surveys and Tutorials*, vol. 12, no. 9, pp. 11 734–11 753, September 2012.

[29] M. Harvan, "Connecting Wireless Sensor Networks to the Internet - A 6lowpan Implementation for TinyOS 2.0," Master's thesis, Jacobs University Bremen, School of Engineering and Science, May 2007.

[30] Hootsuite, "The Global State of Digital in 2019 Report," Jul. 2019 (Zugriff: 29.08.2019). [Online]. Available: https://hootsuite.com/pages/digital-in-2019

[31] J. Hui and P. Thubert, "Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks," RFC 6282 (Proposed Standard), RFC Editor, Fremont, CA, USA, pp. 1–24, Sep. 2011, updated by RFC 8066. [Online]. Available: https://www.rfc-editor.org/rfc/rfc6282.txt

[32] IEEE Standards Association, "IEEE Standard for Low-Rate Wireless Networks," IEEE Computer Society, New York, NY, USA, IEEE Std 802.15.4 - 2015, 2015. [Online]. Available: http://standards.ieee.org/getieee802/download/802.15.4-2015.pdf

[33] ISO/IEC, "Information technology - Advanced Message Queuing Protocol (AMQP) v1.0 specification," ISO/IEC 19464 (Standard), International Organization for Standardization, Technical Committee, ISO/IEC JTC 1 Information Technology, May 2014. [Online]. Available: https://www.iso.org/standard/64955.html

[34] ——, "Information technology - MQ Telemetry Transport (MQTT) v3.1.1," ISO/IEC 20922 (Standard), International Organization for Standardization, Technical Committee, ISO/IEC JTC 1 Information Technology, May 2014. [Online]. Available: https://www.iso.org/standard/69466.html

[35] A. Jules, "RFID Security and Privacy: A Research Survey," *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 2, pp. 381–394, February 2006.

[36] E. Kim, D. Kaspar, C. Gomez, and C. Bormann, "Problem Statement and Requirements for IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) Routing," RFC 6606 (Informational), RFC Editor, Fremont, CA, USA, pp. 1–32, May 2012. [Online]. Available: https://www.rfc-editor.org/rfc/rfc6606.txt

[37] J. Kurose and K. Ross, *Computer Networks - A Top-Down Approach*. Upper Saddle River, NJ, USA: Prentice Hall, October 2016, vol. 7.

[38] N. Kushalnagar, G. Montenegro, and C. Schumacher, "IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals," RFC 4919 (Informational), RFC Editor, Fremont, CA, USA, pp. 1–12, Aug. 2007. [Online]. Available: https://www.rfc-editor.org/rfc/rfc4919.txt

[39] J. Langer and M. Roland, *Anwendungen und Technik von Near Field Communication (NFC)*. Springer Berlin Heidelberg, 2010.

[40] O. Liberg, M. Sundberg, E. Wang, J. Bergman, and J. Sachs, *Cellular Internet of things: technologies, standards, and performance*. Academic Press, 2017.

[41] LoRa Alliance, "LoRa Alliance Homepage," https://www.lora-alliance.org/, last access: April 20, 2020.

[42] E. Macias and J. Wyatt, "NFC Active and Passive Peer-to-Peer Communication Using the TRF7970A," Texas Instruments, Tech. Rep. SLOA1291A, December 2016.

[43] H. Malik, H. Pervaiz, M. Mahtab Alam, Y. Le Moullec, A. Kuusik, and M. Ali Imran, "Radio resource management scheme in nb-iot systems," *IEEE Access*, vol. 6, pp. 15 051–15 064, 2018.

[44] A. Marquet, N. Montavont, and G. Z. Papadopoulos, "Investigating Theoretical Performance and Demodulation Techniques for LoRa," in *2019 IEEE 20th International Symposium on "A World of Wireless, Mobile and Multimedia Networks" (WoWMoM)*, June 2019, pp. 1–6.

[45] C. Miller, "Exploring the NFC Attack Surface," http://media.blackhat.com/bh-us-12/Briefings/C_Miller/BH_US_12_Miller_NFC_attack_surface_WP.pdf, August 2012, last access: April 20, 2020.

[46] L. Oliveira, J. J. Rodrigues, S. A. Kozlov, R. A. Rabêlo, and V. H. C. d. Albuquerque, "MAC layer protocols for internet of things: A survey," *Future Internet*, vol. 11, no. 1, p. 16, 2019.

[47] I. S. Organization, "Information technology - Telecommunications and information exchange between systems - Near Field Communication - Interface and Protocol (NFCIP-1)," International Standard Organization, Geneva, Switzerland, Tech. Rep. ISO/IEC 18092:2013(E), March 2013.

[48] S. Popli, R. K. Jha, and S. Jain, "A survey on energy efficient narrowband internet of things (NBIoT): Architecture, application and challenges," *IEEE Access*, vol. 7, pp. 16 739–16 776, 2018.

[49] J. Postel, "Internet Protocol," RFC 791 (Internet Standard), RFC Editor, Fremont, CA, USA, pp. 1–51, Sep. 1981, updated by RFCs 1349, 2474, 6864. [Online]. Available: https://www.rfc-editor.org/rfc/rfc791.txt

[50] Postscapes, "IoT Technology Guidebook," https://www.postscapes.com/internet-of-things-technologies/, November 3, 2017, last access: April 20, 2020.

[51] ——, "IoT Standards and Protocols," https://www.postscapes.com/internet-of-things-protocols/, February 1, 2020, last access: April 20, 2020.

[52] F. Rayal, "LTE in a nutshell: The physical layer," *Telesystem Innovations*, 2010, https://home.zhaw.ch/kunr/NTM1/literatur/LTE%20in%20a%20Nutshell%20-%20Physical%20Layer.pdf, last access: April 2, 2020.

[53] U. Raza, P. Kulkarni, and M. Sooriyabandara, "Low Power Wide Area Networks: An Overview," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 2, pp. 855–873, 2017.

[54] RF Wireless World, "NFC A vs NFC B vs NFC F-Difference between NFC-A, NFC-B, NFC-F," http://www.rfwireless-world.com/Terminology/NFC-A-vs-NFC-B-vs-NFC-F.html, 2012, last access: April 20, 2020.

[55] M. Roberti, "Internet of Things: Promise and Peril for the RFID Industry," *RFID Journal*, December 1, 2014.

[56] P. Robyns, P. Quax, W. Lamotte, and W. Thenaers, "A Multi-Channel Software Decoder for the LoRa Modulation Scheme," 01 2018, pp. 41–51.

[57] R. H. S. Deering, "Internet Protocol, Version 6 (IPv6)," RFC 2460 (Internet Standard), RFC Editor, Dec. 1988. [Online]. Available: https://www.rfc-editor.org/rfc/rfc2460.txt

[58] E. Schiller, S. Weber, and B. Stiller, "Design and Evaluation of an SDR-based LoRa Cloud Radio Access Network," in *16th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob2020)*, October 2020, p. Session S4.

[59] E. Schiller, N. Nikaein, E. Kalogeiton, M. Gasparyan, and T. Braun, "CDS-MEC: NFV/SDN-based application management for MEC in 5G systems," *Computer Networks*, vol. 135, pp. 96–107, 2018.

[60] J. Schiller, *Mobile Communications*. New York, NY, USA: Addison Wesley, August 2003.

[61] J. Schlienz and D. Raddino, "Narrowband internet of things whitepaper," *White Paper, Rohde&Schwarz*, pp. 1–42, 2016, https://cdn.rohde-schwarz.com/pws/dl_downloads/dl_application/application_notes/1ma266/1MA266_0e_NB_IoT.pdf, last access: April 2, 2020.

[62] C. Schmitt, "Secure Data Transmission in Wireless Sensor Networks," Ph.D. dissertation, Chair for Network Architectures and Services, Technische Universität München, Munich, Germany, July 2013.

[63] C. Schmitt, M. Noack, and B. Stiller, *TinyTO: Two-way Authentication for Constrained Devices in the Internet-of-Things*. Cambridge, MA, USA: Morgen Kaufmann, 2016, p. 239–258.

[64] D. Sen, P. Sen, and A. Das, *RFID For Energy and Utility Industries*. Tusla, OK, USA: PennWell Corp, January 2009.

[65] Z. Shelby and C. Bormann, *6LoWPAN - The Wireless Embedded Internet*. West Sussex, England, UK: Wiley-Blackwell, November 2009.

[66] Z. Shelby, S. Chakrabarti, E. Nordmark, and C. Bormann, "Neighbor Discovery Optimization for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)," RFC 6775 (Proposed Standard), RFC Editor, Fremont, CA, USA, pp. 1–55, Nov. 2012. [Online]. Available: https://www.rfc-editor.org/rfc/rfc6775.txt

[67] Sigfox, "Sigfox," https://www.sigfox.com/en, 2020, last access: April 20, 2020.

[68] R. Silva, J. Silva, and F. Boavida, "Evaluating 6lowPAN implementations in WSNs," in *9th Conferencia sobre Redes de Computadores Oeiras*, Oeiras, Portugal, September 2009, pp. 1–5.

[69] N. Sornin, M. Luis, T. Eirich, T. Kramp, and O. Hersent, "LoRaWAN Specification," LoRa Alliance, Tech. Rep. V1.0.2, July 2016.

[70] Statistica Inc., "The Statistics Portal," November 2017, https://www.statista.com, last access: April 20, 2020.

[71] P. Thubert and R. Cragie, "IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) Paging Dispatch," RFC 8025 (Proposed Standard), RFC Editor, Fremont, CA, USA, pp. 1–8, Nov. 2016. [Online]. Available: https://www.rfc-editor.org/rfc/rfc8025.txt

[72] M. Walters, "Inspectrum: a New Tool for Analysing Captured Signals, https://github.com/miek/inspectrum," last access April 20, 2020.

[73] S. Weis, "RFID (Radio Frequency Identification): Principles and Applications," *MIT Computer Science and Artificial Intelligence Laboratory*, 2007.

[74] M. Weyn, G. Ergeerts, L. Wante, C. Vercauteren, and P. Hellinckx, "Survey of the DASH7 alliance protocol for 433 MHz wireless sensor communication," *International Journal of Distributed Sensor Networks*, vol. 9, no. 12, 2013.

[75] T. Winter, P. Thubert, A. Brandt, J. Hui, R. Kelsey, P. Levis, K. Pister, R. Struik, J. Vasseur, and R. Alexander, "RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks," RFC 6550 (Proposed Standard), RFC Editor, Fremont, CA, USA, pp. 1–157, 2012. [Online]. Available: https://www.rfc-editor.org/rfc/rfc6550.txt

[76] S. Yi, S. Chun, Y. Lee, S. Park, and S. Jung, *Radio Protocols for LTE and LTE-advanced*. John Wiley & Sons, 2012.

[77] Z-Wave, "Z-Wave," https://www.z-wave.com/, 2020, last access: April 20, 2020.

[78] ZigBee Alliance, "ZigBee Specification," ZigBee Standards Organization, Tech. Rep. 53474r20, September 2012.

12.8 Author Biographies



Burkhard Stiller received his diploma degree in computer science (M.Sc.) and his doctoral degree (Dr. rer.-nat.) from the University of Karlsruhe, Germany, in 1990 and 1994, respectively.

From 1991 until 1995 he has been a research assistant at the University of Karlsruhe, being on leave in 1994/95 for a one-year EC Research Fellowship at the University of Cambridge, Computer Laboratory, UK. From November 1995, he has been with the Computer Engineering and Networks Laboratory (TIK) of ETH Zurich. He was appointed assistant professor for Communication Systems at ETH in 1999 and held that post until September 2004. Burkhard held additionally from April 2002 until August 2004 a full professorship at the University of Federal Armed Forces Munich (UniBwM), where he headed the Information Systems Laboratory IIS and had a part-time appointment with ETH Zurich. Since September 2004, Burkhard holds the Communications Chair as a full professor at the University of Zurich UZH, Department of Informatics IfI, leading the Communication Systems Group CSG.

Burkhard participated in or managed national research projects of Switzerland, Germany, and the UK as well as EU IST projects, such as CONCORDIA, SESERV, SmoothIT, SmartenIT, FLAMINGO, EMANICS, Akogrimo, Daidalos, EC-GIN, MMAPPS, Moby Dick, CATI, M3I, CoopSC, DaSaHIT, ANAISOFT, DaCaPo++, and F-CSS, all complemented with industrial projects within Switzerland such as PasWITS, BC4CC, FoodChains, AMAAIS, or DAMMO.

Burkhard's main research interests are published in well over 300 research papers in leading journals, conferences, workshops, and standards, and include systems with fully decentralized control (Blockchains, clouds, peer-to-peer), network and service management (economic management), Internet-of-Things (security of constrained devices, LoRa), and telecommunication economics (charging and accounting).



Eryk Schiller received two diplomas: one M.Sc. in Electronics & Telecommunications from the University of Science and Technology (UST) and one M.Sc. in Theoretical Physics from the Jagiellonian University (JU), Cracow, Poland in 2006 and 2007, respectively. He received a Ph.D. in Computer Science from the University of Grenoble, France, in 2010.

Between 2010 and 2014 he was appointed as a postdoctoral research assistant at the University of Neuchâtel, Switzerland. Between 2014 and 2019 he was with the University of Bern, Switzerland. Since 2018 he is with the Communication Systems Group CSG, at the Department of Informatics IfI, University of Zurich UZH, Switzerland and holds an appointment of a senior researcher.

Eryk is an author of various book chapter, journal, conference, and workshop publications in the domain of communication networks, distributed systems, and cloud computing. Eryk was appointed on a few European projects including IST-WIP, MCN, FLEX, and CONCORDIA as well as national projects of France and Switzerland. His interests center around cloud computing and communication networks.



Corinna Schmitt received a degree of a Diplom-Informatikerin (Bioinformatikerin) from the Eberhard-Karls University of Tübingen, Germany, and her Ph.D. degree (Dr. rer.-nat.) from the Technical University of Munich (TUM), Germany. Currently, she finishes her Habilitation at the University of Zurich UZH, Switzerland, where she was employed as senior researcher for “Mobile and Trusted Communications” at the Communication Systems Group CSG between 2013 and 2018. Since 2018, she is a researcher and the lab manager for “IoT and Mobile Communications" at the Research Institute CODE, Universität der Bundeswehr München, Germany.

Her research focuses on mobile and trusted communications in IoT. Her work is documented in more than 30 publications, including several book chapters, journal articles, and papers as well as standards, such as RFC 8272 and ITU-T recommendation Y.3013. She contributed to several EU projects, such as CONCORDIA, symbIoTe, SmartenIT, FLAMINGO, and AutHoNe, and different standardization organizations, including IETF, ITU, and ASUT. She is active within ACM and IEEE, as a TPC member, as a reviewer for several journals and funding schemes, and as an organizer of conferences.

12.9 Index

1G, 3, 13, 21
2.5G, 13
2G, 13
3G, 13
3GPP, 3, 13, 14, 17, 18, 20, 21
3rd Generation Partnership Project, 13
4G, 12, 13, 21
5G, 2, 3, 12, 13, 21
6LoWPAN, 2, 3, 5–7, 21

Advanced Encryption Standard, 6
Advanced Message Queuing Protocol, 2
AES, 6, 7, 10
Alljoyn, 2
AMQP, 2, 3
APS, 6
ARQ, 15
AS, 1
Automatic Repeat reQuest, 15
Autonomous System, 1

Base Station, 12
Base Station Controller, 12
Base Transceiver Station, 12
Berkeley Low-power IP, 2, 7
Binary Phase Shift Keying, 20
BLIP, 2, 5–7, 21
Bluetooth, 2, 3, 11, 12, 21
Bluetooth Low Energy, 12
BPSK, 20
Broadband Forum, 2
Broadband Forum Technical Report 069, 2
BS, 12
BSC, 12
BTLE, 12
BTS, 12

Carrier Sense Multiple Access, 5
    Collision Avoidance, 5
CDMA, 13
CE, 18, 19
Channel Quality Information, 19
CoAP, 2, 3
Code Division Multiple Access, 13
Constrained Application Protocol, 2
Coverage Enhancement, 18
CQI, 19
CSMA
    CA, 5, 7, 10

D7A, 10
DASH7, 3, 10, 21
    Alliance, 10
Data Distribution Service, 3
DBPSK, 7
DDS, 3
Device Management, 2
Differential Binary Phase-Shift Keying, 7
Discontinuous Reception, 16
DNS-SD, 2
DRX, 16, 18, 20

EC-GSM-IoT, 14
EDGE, 13
eDRX, 20
eNB, 14–20
Enhanced Data Rates for GSM Evolution, 13
evolved Node B, 14
Extended DRX, 20

FDMA, 13, 16, 18, 20
FEC, 9, 10, 15–17
FFD, 5
Forward Error Correction, 9, 15
Frequency-Division Multiple Access, 13
Full Functional Device, 5

Gaussian Frequency Shift Keying, 7
Gaussian Frequency-Shift Keying, 10
General Packet Radio Service, 13
GFSK, 7, 10
GPRS, 13
GSM, 4, 13, 20

HARQ, 15, 16, 19
High Speed Downlink Packet Access, 13
High-speed Curcuit-switched Data Service, 13
HSCDS, 13
HSDPA, 13
Hybrid Automatic Repeat reQuest, 15

IEEE 802.11, 2–5, 21
IEEE 802.15.1, 11
IEEE 802.15.4, 2–7, 21
IEEE 802.3, 3
IETF, 6
Industrial, Scientific, and Medical, 5
Institute of Electrical and Electronics Engineers, 2
Inter Symbol Interference, 16
Internet Engineering Task Force, 6
IoTivity, 2
ISI, 16
ISM, 5, 7, 8, 10, 11

JavaScript Object Notation for Linked Data, 2
JSON-LD, 2

LAN, 2–4, 12, 13, 21

Local Area Network, 3
Long Term Evolution, 2, 13
Long-Range, 2, 7
Long-Range Wide Area Networks, 7
LoRa, 2, 3, 7–10, 21
    Alliance, 7
LoRaWAN, 7, 8
LTE, 2–4, 12–14, 16, 17, 19–21
    Advanced, 13, 17, 21
    Advanced Pro, 18, 21
    Cat. 0, 14, 18, 21
    Cat. 1, 17
    Cat. 14, 18
    Cat. 5, 17
    Cat. 6, 17
    Cat. 8, 17, 21
    Cat. M, 13, 14, 18–21
    Cat. M1, 18, 21
    Cat. N, 13, 14, 18, 20, 21
    Category 0, 14
    Category M, 13, 14
    Category N, 13, 14
    Frequency Division Duplex, 16
    Time Division Duplex, 16
LTE-A, 13, 17, 18
LTE-FDD, 16, 18
LTE-TDD, 16–18
LTE-Uu, 14

MAC, 2–8, 10, 11, 15, 16
Machine Type Communication, 19
MAN, 13
Maximum Transmission Unit, 5
mDNS, 2
Medium Access Control, 2, 3
Message Queuing Telemetry Transport, 2
Metropolitan Area Network, 3
MIMO, 13, 17, 18
MNO, 14
Mobile Network Operator, 14
Mobile Switching Centers, 12
MQTT, 2, 3
MSC, 12
MTC, 19
MTU, 5, 7
Multicast Domain Name System, 2
Multiple-Input and Multiple-Output, 13

NB-IoT, 13, 14, 20
Near Field Communication, 2, 11
NFC, 2, 3, 11, 21
    Forum, 11
NFC-A, 11
NFC-B, 11
NFC-F, 11

Object Management Group, 3
OFDM, 16, 17, 20
OFDMA, 13, 16, 18, 20
OMA, 2
OMA-DM, 2
OMG, 3
Open Mobile Alliance, 2
Orthogonal Frequency-Division Multiple Access, 13, 16
Orthogonal Frequency-Division Multiplexing, 16

Packet Data Convergence Protocol, 14
PAN, 2–4, 11–13, 21
PDCP, 14, 15
Personal Area Network, 3
PHY, 2, 11, 14–16, 18–21
Physical Resource Block, 16
piconet, 11, 12
PRB, 16–20
PSTN, 12, 13
Public Switched Telephone Network, 12

QAM, 17–19
QPSK, 17–20
Quadrature Amplitude Modulation, 17
Quadrature Phase-Shift Keying, 17

Radio Access Network, 14
Radio Frequency Identification, 2, 10
Radio Frequency Identifier, 5
Radio Link Control, 15
Radio Resource Control, 14
RAN, 14
Reduced Functional Device, 5
RFD, 5
RFID, 2, 3, 5, 10, 11, 21
RLC, 15
RRC, 14, 15, 18

Sigfox, 7
Signal-to-Noise, 14
Single Input Single Output, 17
SISO, 17, 18
SNR, 14

TCP, 5–7
TDMA, 13
The Things Network, 8
Time-Division Multiple Access, 13
TR-069, 2
Transmission Control Protocol, 5
Transmission Time Interval, 17
TTI, 17–19

TTN, 8

UDP, 6, 7
UE, 14–20
UMTS, 2, 4, 13
Universal Mobile Telecommunication System, 13
Universal Mobile Telecommunications Service, 2
User Datagram Protocol, 6
User Equipment, 14

W-CDMA, 13
WAN, 2, 3, 12, 13, 21
Wide Area Network, 2, 3
Wideband-CDMA, 13
Wireless Personal Area Networks, 3
Wireless Sensor Network, 4
WPAN, 3, 5
WSN, 4–6, 10

Z-Wave, 10, 11, 21
    Alliance, 11
ZDO, 6
ZigBee, 2, 3, 5–7
    Alliance, 6
    Application Support Sub-Layer, 6
    Device Objects, 6