1

IoT Technologies and Applications

1.1 Introduction

As a new dimension to the world of information and communication technologies (ICTs), the concept of the internet of things (IoT) aims at providing "connectivity for anything", "by embedding short-range mobile transceivers into a wide array of additional gadgets and everyday items, enabling new forms of communication between people and things, and between things themselves", according to the seventh International Telecommunication Union (ITU) Internet Reports 2005 (International Telecommunication Union (ITU), 2005). In recent years, different IoT technologies and standards have been actively developed for different industrial sectors and application scenarios, such as smart city, intelligent transportation system, safety, and security system, intelligent agriculture, environment monitoring, smart factory, intelligent manufacturing, smart home, and healthcare. Various IoT-centered business models and value chains have become, consolidated, and popular; these IoT applications are effectively accelerating the digitalization and transformation progresses of traditional industries (Union, 2016). As a result, they have generated tremendous economic and social benefits to our society, as well as huge impacts on people's daily life.

Sensors, machines, and user devices are the "things", which are usually equipped with limited energy resources and simple sensing, computing, communication, motion, and control capabilities. By using a large number of sensors in the field, a typical IoT system can effectively expand its service coverage and capability in sensing, collecting, and processing different types of raw data obtained from the physical world. Most redundant data with low value will be aggregated or filtered for saving scarce communication resources, i.e. bandwidth, storage,and energy. Selected data with potential values, e.g., characteristics of unexpected events, will be transmitted from different sites through multi-hop communication networks to a centralized computing facility, such as a data center, for further in-depth investigation. New information will be extracted, or new events will be discovered, from this more comprehensive analysis of massive data from a much larger area across multiple sites and locations.

In the early days, IoT systems were usually developed according to rigid rules or requirements. The main purpose is to improve the perception of the physical world, as well as the efficiency of data collection and analysis, in different IoT applications such as environment monitoring and emergency management. As a well-known application-driven IoT architecture, the ISO/IEC 30141-IoT Reference Architecture is often adopted in system designs

Intelligent IoT for the Digital World: Incorporating 5G Communications and Fog/Edge Computing Technologies, First Edition. Yang Yang, Xu Chen, Rui Tan, and Yong Xiao.

and service deployments (Union, 2016). Data acquisition involves all kinds of sensors, such as RFID, MEMS, bar code, and video camera. However, due to dynamic application scenarios and environments, the key function and challenge for IoT systems are high-quality data collection (transmission) through wireless ad hoc networks. Many wireless access and networking technologies have been developed for ensuring timely and reliable connectivity and transmission for data collection at low cost and low energy consumption (Yang et al., 2006b,a, Zhao et al., 2015). In addition to the existing standards for mobile communications, the internet, and broadcasting networks, a series of wireless communication technologies have been developed for supporting IoT data transmissions in various application scenarios, e.g. RFID, Wi-Fi, NFC, ZigBee, LoRa, and Sigfox (Jia et al., 2012, Li et al., 2011, Vedat et al., 2012, Alliance, 2012, Augustin et al., 2016, Sigfox, 2018a). By collaboratively analyzing data from multiple sensors in different areas, a more comprehensive perception of the actual environment and a timely understanding of the exact situation will be achieved, thus enabling better decision making and performance optimization for particular industrial operations.

Nowadays, a series of advanced technologies on smart sensing, pervasive computing, wireless communication, pattern recognition, and behavior analysis have been widely applied and integrated for supporting more and more sophisticated IoT applications, such as intelligent transportation system and intelligent manufacturing. Such complex applications can significantly improve system automation and efficiency in massive data analysis and task execution. To achieve this goal, the key function and challenge for IoT systems is accurate information extraction, which heavily depends on domain-specific knowledge, valuable experience, and technical know-how contributed by real experts and field workers. In order to make IoT systems more accessible and deployable, the fourth-generation (4G) and fifth-generation (5G) mobile communication standards have specified several important IoT application scenarios, i.e. Narrowband IoT (NB-IoT) in 4G massive Machine Type Communications (mMTC) and ultra-reliable and low latency communications (URLLC) in 5G (3GP, 2017, 3GPP, 2016a, Yang et al., 2018). Furthermore, the latest developments in cloud computing and big data technologies enable fast and accurate analysis of huge volumes of structured and non-structured data, creating lots of business opportunities for the development of more sophisticated and intelligent IoT systems. The continuous progression and widespread deployment of IoT technologies have been transforming many industrial sectors and commercial ecosystems. Now, IoT applications and services are becoming indispensable to our daily lives and business models, e.g., remote control of door locks, lights, and appliances at homes and offices, real-time modeling of resource consumption patterns and streamline business processes in factories, constant surveillance for property security, public safety and emergency management in cities.

To meet the fast-growing demands of various IoT applications and services for different businesses and customers, leading ICT companies, such as Amazon, Google, Microsoft, Cisco, Huawei, Alibaba, and JD, have launched their own cloud-based IoT platforms for data-centric services. However, these enterprise-level platforms are not designed for data sharing, nor service collaboration. General concerns of data security and customer privacy strictly prevent the attempts of connecting and integrating them for much bigger commercial benefits and global influences. Besides, it is even harder to overcome the existing

barriers of vertical industries and realize cross-domain information exchanges for minimizing the redundancies and fragments at different but related IoT applications.

In the future, when artificial intelligence (AI) technologies are widely adopted in most industrial sectors and application domains, new links will be established between those domain-specific island-like solutions. In most cases, they are not used to share original data, but only to exchange necessary knowledge that is purposely learned from separated/protected datasets for customized applications. To realize this ambitious vision, the key function and challenge for future IoT systems is innovative knowledge creation, which requires high-quality data, super-intelligent algorithms, and more computing resources everywhere. Centralized cloud computing alone cannot support this fundamental change, while dispersive fog computing technologies will fill the computational gap along the continuum from cloud to things. Therefore, future intelligent IoT systems will fully utilize the best available computing resources in their neighborhood and in the cloud to calculate novel effective mechanisms and solutions, which are acceptable and executable across different enterprise platforms, industrial sectors, and application domains. In this way, those domain-specific IoT systems are not closed or isolated any more, they will become much more powerful and influential by working collaboratively, thus significantly saving global resources, improving overall performance, and maximizing potential benefits in all systems. There is no doubt that future IoT applications and services will be shifting from data-centric to knowledge-centric. Very soon, they will become better than human-designed ones, since they are taught by us and powered by accumulated data, sophisticated AI algorithms, endless computing resources, and fast evolution. Eventually, they will help us not only search and identify useful information from massive raw data, but more importantly, discover, and create new knowledge to expand our horizons and capabilities.

The rest of this chapter is organized as follows. Section 1.2 reviews some well-known and emerging IoT standards and technologies. Section 1.3 introduces intelligent IoT technologies, including an intelligent user-centered IoT network, in which data, computing power, and intelligent algorithms are distributed around its users. Typical IoT applications are summarized in Section 1.4. New requirements and challenges of IoT systems are analyzed in Section 1.5. Finally, Section 1.6 concludes this chapter.

1.2 Traditional IoT Technologies

1.2.1 Traditional IoT System Architecture

The IoT is a platform where every day devices become smarter, every day processing becomes more intelligent, and every day communication becomes more informative. While the IoT is still seeking its own shape, its effects have already started in making incredible strides as a universal solution media for the connected scenario. Architecture specific study does always pave the conformation of the related field. IoT is a dynamic global network infrastructure with the capability of self-configuring based on standards and interoperable protocols. IoT enables physical and virtual “things” to use intelligent interfaces and seamlessly integrate into an information network (van Kranenburg and Dodson, 2008).

A multi-layer technology is used to manage the connected "things" is known as the IoT system. It brings the physical or virtual devices to the IoT network, and provides the various services to the devices by using machine to machine communication. An traditional IoT system architecture is comprised of various functional layers to enable IoT applications, including asensing layer, network layer, and application layer. This section will introduce these functional layers.

1.2.1.1 Sensing Layer

The sensing layer plays the role of interface between the physical world and information world, and is the foundation of IoT. This layer consists of a physical layer system such as smart sensors and devices, and communicates with the network layer. The main function is to identify and track objects. To achieve this function, several technologies including RFID, bar code technology, sensor technology, positioning technology, or other information sampling technology can be implemented. With the development of science and technology, sensors are becoming more and more intelligent. The smart sensors have numerous advantages over conventional sensors, such as low cost and power, flexible connection, high-reliability band efficient, and less cable communication. IoT systems are based on the data that provide actuation, control, and monitoring activities. IoT devices can exchange data with other connected devices and applications, or collect data from other devices. They can also process the data locally, or send the data to a centralized server or use cloud-based servers to process the data. They can perform some tasks locally and other tasks within IoT infrastructure based on temporal and spatial constraints (i.e. memory, processing capabilities, communication latencies, and speeds, and deadlines). IoT devices may contain multiple interfaces for communicating with other devices (wired and wireless). IoT devices can also be of many types, such as wearable sensors, smart watches, LED lights, cars, and industrial machines. IoT devices and systems should have the ability to dynamically adapt to changing environments and take actions based on their operating conditions, user environment or perceived environment. For example, consider a pollution surveillance system consisting of multiple sensor nodes. Existing IoT supports different hardware platforms, such as Arduino, Intel Galileo Gen, Intel Edison, Beagle Bone Black, and Raspberry Pi. The platforms are classified according to key parameters, including processor, GPU, operating voltage, clock speed, bus width, system memory, flash memory, EEPROM, supported communications, development environment, programming language, and I/O connection. For example, the Arduino Uno platform supports a lightweight system with 2 KB of memory, which can be used to build sensor networks economically. Intel Edison has provided better performance, which can support 1 GB system memory and could support more applications flexibly.

1.2.1.2 Network Layer

The network layer performs communication between the device and a remote server. The IoT environment consists of an enormous number of smart devices, but with many constraints. Limited processing capability, storage volume, battery life, and communication range are among of these constraints. Therefore, the IoT implementation requires a communication protocol that can efficiently manage these conditions (Al-Sarawi et al., 2017, Farhan et al., 2017).

The protocols form the backbone of IoT systems, and enable network connection and coupling with application programs. Communication protocols allow devices to exchange data over a network. The protocols define data exchange format, data encoding, device addressing scheme, and routing of packets from source to destination. Other functions of the protocols include sequence control, flow control, and retransmission of lost packets. There are many wireless communication technologies with various parameters (Ahmed et al., 2016, Madakam et al., 2015). The communication technology of IoT can operate in sensor and backhaul network scenarios. Sensor network standards (such as ZigBee, RFID or Bluetooth) work over relatively short distances (i.e. tens of meters), with low data rates and low energy consumption. On the other hand, standards such as GPRS, LTE, WiMAX can work over long distances and provide high throughput. However, they consume more energy, require expensive and fixed base station infrastructure with proper communication connectivity (Lee and Kim, 2016, Ahmed et al., 2016).

IEEE 802.11: 802.11 is a collection of wireless local area network (WLAN) communication standards for wi-fi. For example, 802.11a operates in the 5 GHz band, 802.11b and 802.11g operate in the 2.4 GHz band, 802.11n operates in the 2.4/5 GHz bands, 802.11ac operates in the 5 GHz band, and 802.11ad operates in the 60 GHz band. These standards provide data rates from 1 Mb s^{-1} to 6.75 Gb s^{-1}. Wi-fi provides a 20 m indoor communication range and 100 m in the outdoors (Ray, 2018). The emerging IEEE 802.11ah is a promising communication standard that supports a massive number of heterogeneous devices in the IoT. It provides attractive features like improved scalability, low energy consumption, and large coverage area. In this chapter, the authors analyze the performance of IEEE 802.11ah, and compare it with a prominent alternative, the IEEE 802.15.4. The simulation results show that the new 802.11ah standard performs better than the 802.15.4 in terms of association time, throughput, delay, and coverage range (Hazmi et al., 2012).

IEEE 802.15.4: 802.15.4 is a collection of low-rate wireless personal area network (LR-WPAN) standards. It can be contrasted with other approaches, such as Wi-Fi, which offers more bandwidth and require more power. The emphasis is on very low-cost communication of nearby devices with little to no underlying infrastructure, intending to exploit this to lower power consumption even more. LR-WPAN standards provide data rates from 40 Kb s^{-1} to 250 Kb s^{-1}. These standards provide low-cost and low-speed communication to power-constrained devices. They operate at 868/915 MHz and 2.4 GHz frequencies at low and high data rates, respectively. Important features include real-time suitability by reservation of guaranteed time slots (GTS), collision avoidance through CSMA/CA, and integrated support for secure communications. Devices also include power management functions such as link quality and energy detection. The standard does have provisions for supporting time and rate sensitive applications because of its ability to operate in pure CSMA/CA or TDMA access modes (Pasolini et al., 2018).

Mobile communication: There are different generations of mobile communication standards. 2G is short for second-generation wireless telephone technology. One of the benefits of 2G is that 2G signals consume less battery power, so they help mobile batteries to last longer. Digital coding improves the voice clarity and reduces noise in the line. 2G digital signals are considered environment friendly. The use of digital data service assists mobile network operators to introduce short message service over the cellular phones. Digital encryption has provided secrecy and safety to the data and voice calls. The use of

2G technology requires strong digital signals to help mobile phones work. 3G is the third generation of mobile phone standards and technology, superseding 2G, and preceding 4G. It is based on the International Telecommunication Union (ITU) family of standards under the International Mobile Telecommunications programme, IMT-2000 (Bhalla and Bhalla, 2010). 3G was launched in Japan on October 2001 by NTT DoCoMo. 3G provided a good experience for the mobile user, and supports higher speed connection than the previous generations (and, 2014). The essential factor of this technology is to merge the wireless principles like time division multiple access (TDMA), a global system for mobile communication (GSM) and code division multiple access (CDMA). 4G refers to the fourth generation of cellular wireless standards. It is a successor to 3G families of standards. The nomenclature of the generations generally refers to a change in the fundamental nature of the service, non-backwards compatible transmission technology, and new frequency bands. IoT devices based on these standards can communicate over cellular networks. Data rates for these standards range from 9.6 Kb s^{-1} (2G) to 100 Mb s^{-1} (4G), which are available from the 3GPP websites. 5G is the next generation cellular network that aspires to achieve substantial improvement on quality of service, such as higher throughput and lower latency. 5G wireless system can bring as much as 1000 and above times the capability offered by today's mobile world.

1.2.1.3 Application Layer

The application layer supports various IoT applications, which can transitionally be deployed on cloud platforms. IoT cloud platforms are designed to be meant for particular application specific domains, such as, application development, device management, system management, heterogeneity management, data management, analytics, deployment, monitoring, visualization, and finally research purposes. An IoT system serves various types of functions such as services for device modeling, device control, data publishing, data analytics, and device discovery. Management block provides different functions to govern an IoT system to seek the underlying governance of an IoT system. A security functional block secures the IoT system by providing functions such as authentication, authorization, and privacy. The application layer is the most important one in terms of users as it acts as an interface that provides various functions to the IoT system. The application layer allows users to visualize and analyze the system status at the current stage of action, and sometimes predict futuristic prospects. It is obvious that there are many more platforms currently present in the market, such as the Google Cloud Platform, Microsoft Azure IoT Suite, IRI Voracity, Particle, ThingWorx, IBM Watson IoT, and Amazon AWS IoT Core. For example, Google Cloud provides a multi-layered secure infrastructure. It helps in improving operational efficiency. It provides predictive maintenance for equipment, solutions for smart cities and buildings, and real-time asset tracking. The Microsoft Azure IoT solution is designed for different industry needs. It can be used from manufacturing to transportation to retail. It provides solutions for remote monitoring, predictive maintenance, smart spaces, and connected products.

Available architectures explore multiple opportunities to seek the advantageous part of IoT while encouraging the developer and user groups to get application specific solutions. However, the central issue of these architectures is the lack of full interoperability of interconnected things at the abstraction level. This leads to many proclaimed problems, such as

degraded smartness of high degree, less adaptability, limited anonymity, poor behavior of the system, reduced trust, privacy, and security. IoT architectures do pose several network oriented problems due to their limitations in a homogeneity approach.

1.2.2 IoT Connectivity Technologies and Protocols

The IoT refers to the inter connection and exchange of data among devices/sensors. Currently, with the explosive growth of IoT technologies, an increasing number of practical applications can be found in many fields, including security, asset tracking, agriculture, smart metering, smart cities, and smart homes. Short-range radio technologies e.g., radio-frequency identification (RFID), near field communication (NFC), and ZigBee are widely used for building automation, automotive, and monitoring devices. For example, wi-fi based on the IEEE 802.11 standards are used in most office environments. However, short-range radio technologies are not adapted for scenarios that require long range transmission.

Cellular networks are widespread and ubiquitous, covering 90% of the world's population, and other technologies like wi-fi don't have the same scale, requiring users to search for and connect to a local network. RF providers, and wireless infrastructure companies and carriers have made massive investments in cellular networks to provide a secure and reliable service to as many customers as possible. By leveraging existing infrastructure and mature technology, cellular IoT can connect millions of IoT devices with little additional investment. Solutions based on cellular communications (e.g., 2G, 3G, and 4G) can provide larger coverage, but they consume excessive energy.

IoT application requirements have driven the emergence of a new wireless communication technology: low power wide area network (LPWAN) (Mekki et al., 2019). LPWAN is increasingly gaining popularity in industrial and research communities because of its low-power, long-range, and low-cost communication characteristics. It provides long-range communication up to 10–40 km in rural zones and 1–5 km in urban zones. In addition, it is highly energy efficient (i.e. 10+ years of battery lifetime) and inexpensive, with the low cost of a radio chip-set (Mekki et al., 2019). In summary, LPWAN is highly suitable for IoT applications that only need to transmit tiny amounts of data in long range. Many LPWAN technologies have arisen in the licensed as well as unlicensed frequency bandwidth. Among them, Sigfox, LoRa, and NB-IoT are today's leading emergent technologies that involve many technical differences(Mekki et al., 2019).

A myriad of IoT connectivity solutions are available to support a wide range of IoT applications with miscellaneous requirements. Therefore, in order to select an optimal technology for each application, various factors, such as power consumption, security issues, deployment cost, communication range, data rate, and latency, are required to be considered. A comparison of some typical IoT connecting solutions (i.e. RFID, NFC, Zigbee, LoRa, Sigfox, and NB-IoT) using a pre-specified factor is given in Table 1.1.

The three main technical requirements for any enterprise looking into IoT connectivity technology are coverage, energy efficiency, and data rate. No single technology can excel in all these aspects, as they are conflicting objectives and every radio technology has to make trade-offs. All IoT applications need good coverage to connect the devices but some need to cover only certain indoor areas while others require extensive coverage in rural or remote regions. A technology with long range is better suited to connecting devices scattered in a

Table 1.1 Comparison of IoT connecting technologies.

Technology	RFID	NFC	BLE	Zigbee	6LoWPAN	LoRa	Sigfox	NB-IoT	MIOTY
Range	1–5 m	1–10 cm	1–10 m	75–100 m	100 m	2–15 km	3–50 km	10–15 km	15–20 km
Bandwidth	2–26 MHz	14 kHz	1–2 MHz	2 MHz	3 MHz	<500 kHz	100 Hz	180 kHz	200 kHz
Frequency band	125–134.2 kHz, 13.56–433 MHz, 860–960 MHz	13.56 MHz	2.4GHz	868 MHz, 915 MHz, 2.4 GHz	2.4 GHz, Sub GHz	868 MHz, 915 MHz, Sub 1 GHz	915–928 MHz, Sub 1 GHz	700 MHz, 800 MHz, 900 MHz	133–966 MHz
Data rate	4–640 kbps	100–424 kbps	1 Mbps	250 kbps	250 kbps	50 kbps with FSK	Less than 100 bps	200 kbps	Sub 1 kbps
Latency	1–10 ms	100 ms	6 ms	~15 ms	2–6 ms	1–10 ms	10–30 ms	40 ms–10 s	10 ms–10 s
Modulation scheme	OOK, FSK, PSK	ASK	DQPSK, DPSK	O-QPSK	QPSK, BPSK	FSK	GFSK, DBPSK	BPSK, QPSK	BPSK, MSK
Battery lifetime	Battery free	Battery free	1–5 days	1–5 years	1–2 years	< 10 years	< 10 years	> 10 years	up to 20 years
Application	Materials management, attendee tracking	Payment, ticketing	IoT device authentication, localization	Smart home, healthcare	Smart city infrastructures	Air pollution monitoring, fire detection	Smart meter, pet tracking	Street lightning, agriculture	Dense IoT network scenarios, smart city
Advantages	High speed and convenience, and very low cost	Convenient to use	Supported by most smartphones	Highly reliable and scalable	Massive connection without complex routing	Highly immune to interference, adaptive data rate	High reliability, low device complexity	Better coverage range and coverage	Low packet error rate, high energy efficiency
Limitation	Brings security and privacy concerns	Limited data rates	Limited range and battery life	Short range, communication security issues	Limited range and data rages	Longer latency, not acknowledges all packets	Multiple transmissions, suffer from interference	No hand-off support, low interference immunity, lacks in ACK	Low data rate
Standard body	ISO/IEC	ISO/IEC	Bluetooth SIG	ZigBee Alliance	IETF	LoRa Alliance	Sigfox	3GPP	MIOTY Alliance

wide area. The energy efficiency of a connectivity technology has a significant impact on the lifetime or the maintenance cycle of IoT devices relying on battery or energy harvesting and is dependent on range, topology and complexity of the connectivity technology. The overall energy consumption of the device also depends on the usage of the application, such as the frequency and duration of message transmission. Data rate requirements for IoT applications vary from hundreds of bit per second (bps) for metering to several megabits per second (Mbps) for video surveillance. In this section, we will introduce traditional IoT connectivity technologies from two categories, low-power and short-range connectivity technologies, and low data rate and wide-area connectivity technologies. Low-power and short-range connectivity technologies include RFID, NFC, Zigbee, and BLE. Low data rate and wide-area connectivity technologies include 6LoWPAN, Sigfox, LoRa, and NB-IoT. Then, we will introduce several emerging IoT technologies, which improve the performance of IoT connectivity in various aspects, such as latency and accessibility. Finally, we will introduce requirements and challenges for intelligent IoT services from the perspective of network provider and users.

1.2.2.1 Low-power and Short-range Connectivity Technologies

Radio Frequency IDentification

The roots of radio frequency identification (RFID) date back to World War II. Germans, for instance, used an interesting maneuver in which their pilots rolled their planes as they return to base, so it would change the reflecting radio signal. This simple procedure alerted the ground radar crew of German planes returning and not allied aircraft. It can be considered one of the first passive ways to identify an object by means of a radio frequency signal, which was known as "identify friend or foe (IFF)". In the 1960s and 1970s, RFID systems were still embedded within the context of "secret technology". As an example, Los Alamos National Laboratory was asked by the Energy Department of United States of America to develop a system for tracking nuclear materials and control sensitive materials. In the 1990s, MIT's Auto-ID Center developed the global standard for RFID and other sensors, which described the IoT as a system where the internet is connected to the physical world through ubiquitous sensors. In the 2010s, the decreased cost of equipment and tags, increased performance to a reliability of 99.9% and a stable international standard brought a major boost in the use of RFID systems.

There are two major initiatives regarding RFID standardization: the International Standard Organization (ISO) and EPCglobal. The ISO uses a cross-industry perspective with a generic approach. Meanwhile EPCglobal adopts a more application-specific approach. The widely recognized outcome of EPCglobal is the establishment of the electronic product code (EPC), a unique code for item numbering, for identification of objects by using a similar approach to barcode numbering. ISO works closely with International Electro-technical Commission (IEC) which is responsible for a general type of RFID standards covering issues of air interface, data content, conformance, and performance. ISO/IEC standards cover certain areas of technology. For instance, ISO 18000 is a series of standards that define air interface standards consisting of channel bandwidth, EIRP, modulation, data coding, and bit rate, and ISO 15418 is a standard that defines data content. There are also many separate standards that had already been developed for livestock tracking (ISO 11785, ISO 11784 and ISO 14223) (Jia et al., 2012, Adhiarna and Rho, 2009).

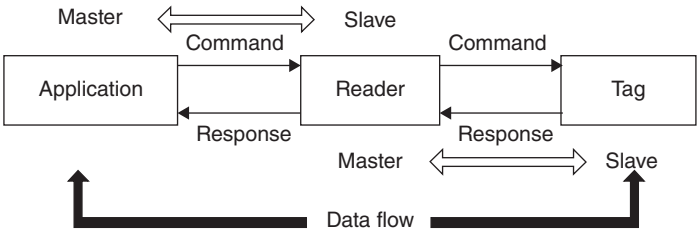

Figure 1.1 The architecture of an RFID system.

A typical RFID system consists of three main components: RFID tags, reader, and an application system (Finkenzeller, 2010, Jia et al., 2012), as shown in Figure 1.1. RFID uses electromagnetic fields to automatically identify and track tags attached to objects. The tags contain electronically stored information. The RFID tags are known as transponders (transmitter/responder), which are attached to the objects to count or identify. Tags could be either active or passive. Active tags are those that have partly or fully battery powered, have the capability to communicate with other tags, and can initiate a dialogue of their own with the tag reader. Passive tags collect energy from a nearby RFID reader's interrogating radio waves. Active tags have a local power source (such as a battery) and may operate hundreds of meters from the RFID reader. Tags consist mainly of a coiled antenna and a microchip, with the main purpose of storing data. The reader is called as transceiver (transmitter/receiver) made up of a radio frequency interface (RFI) module and control unit. Its main functions are to activate the tags, structure the communication sequence with the tag, and transfer data between the application software and tags. The application system is known as data processing system, which can be an application or database, depending on the application. The application software initiates all readers and tags activities. RFID provides a quick, flexible, and reliable way for electronically detecting, tracking, and controlling a variety of items. RFID systems use radio transmissions to send energy to a RFID tag while the tag emits a unique identification code back to a data collection reader linked to an information management system. The data collected from the tag can then be sent either directly to a host computer, or stored in a portable reader and up-loaded later to the host computer.

RFID technology has many advantages. The RFID tag and reader should not have LOS to make the system work, and a RFID reader is capable of scanning multiple tags simultaneously. Unlike barcodes, RFID tags can store more information. Moreover, it follows the instructions/commands of the reader, and provides the location to the reader along with its ID. RFID technology is versatile in nature and hence smaller and larger RFID devices are available as per application. Tags can be read only as well as read/write, unlike barcodes. However, RFID technology also has disadvantages. Active RFID is costly due to the use of batteries. Privacy and security are concerns with the use of RFID on products as it can be easily tapped or intercepted. RFID devices need to be programmed which requires some time. The external electromagnetic interference can limit the RFID remote reading. The coverage range of passive tags is limited to around 3 m.

RFID takes the market in many different areas including inventory management, personnel, asset tracking, controlling access to restricted areas, supply chain management, and counterfeit prevention. The addition of other sensors around AIDC (automated

identification and data capture) technologies such as infrared detectors, radiation, humidity, and others in RFID applications contributed to the development of IoT by extending it to reach intelligent services and providing local capabilities for actuation. For example, in manufacturing, RFID technology offers many applications in the automotive industry. The RFID-based anti-theft device is a protection device installed in many vehicles. RFID also offers great promise for the assembly and manufacturing process of automobiles, especially for flexible and flexible production planning, spare parts, and inventory management. RFID technology not only helps automate the overall assembly process, but also significantly reduces costs and shrinkage, and provides better service for automotive users, including more efficient replacement parts ordering and automatic generation of maintenance reminders. The benefits that RFID brings to the automotive industry, including production processes and end users, are visibility, traceability, flexibility, and enhanced security. In the supply chain, managers will be able to monitor the status of shipments like a crate filled with fruit. With sensors, RFID tags, and RFID readers, the manager sees the exact location of the crate inside the warehouse, the fruit's point of origin, days until expiration, and temperature in real-time. A visible, and transparent process improves efficiency, reduces waste, and allows traceability. If a shipment is determined to be unsuitable for consumption due to disease or other circumstances, the source or cause of the defection will quickly be discovered because of the great wealth of information available.

In summary, the adoption of RFID is spurring innovation and the development of the IoT, which are commonplace throughout households, offices, warehouses, parks, and many other places. Industry and government mandates are regulating RFID technologies leading to accepted standards across industries allowing for interoperability among devices. Additionally, the cost and size of devices continue to decrease which allows companies to embed smaller, common items with RFID chips and sensors. Although promising, RFID is not without its challenges, which arise from electromagnetic interference, security, and privacy issues. Communication between tags and readers are inherently susceptible to electromagnetic interference. Simultaneous transmissions in RFID lead to collisions as readers and tags typically operate on the same wireless channel. Therefore, efficient anti-collision protocols for identifying multi-tags simultaneously are of great importance for the development of large-scale RFID applications Due to its cost and resource constraint limitations, RFID systems do not have a sufficient security and privacy support. Many researchers and scientists work to implement low cost security and privacy protocol to increase the applicability. Lots of lightweight solutions have been proposed for RFID, but they are still expensive and vulnerable to the security and do not fully resolve the security issues.

Near Field Communication

Near field communication (NFC) is a short-range wireless communication technology. NFC technology uses magnetic coupling to send and receive signals. When two NFC enabled devices are close enough (from touch to 10 cm), they create an electromagnetic field between them. That electromagnetic field allows active NFC devices to power up and communicate with the passive NFC device. The active NFC device then picks up on variations in signal levels specific to the passive device and reads those variations as a signal. A detector and decoder circuit in the active NFC device is then used to comprehend

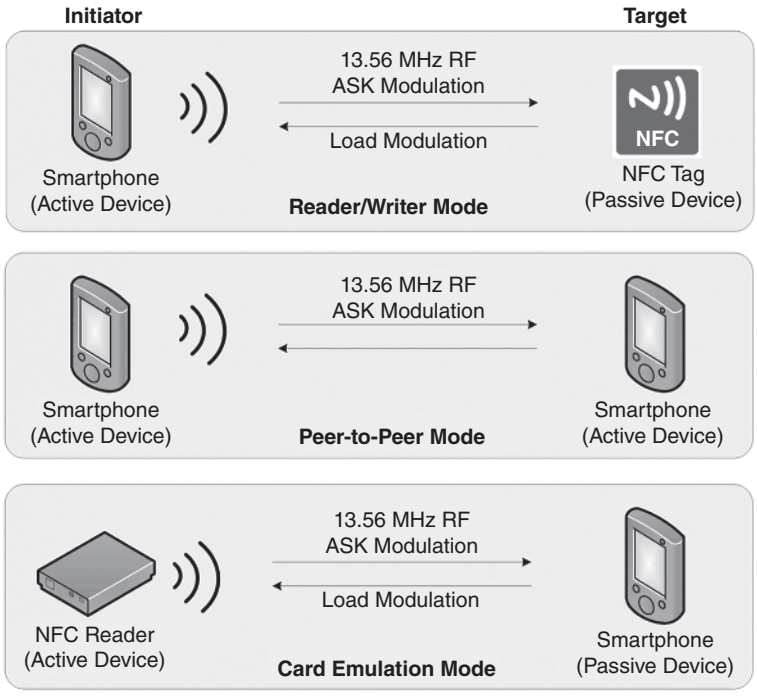

Figure 1.2 NFC system architecture. Source: Vedat Coskun, Busra Ozdenizci, and Kerem Ok. The survey on near field communication. Sensors, 15(6):13348–13405, jun 2015. doi: 10.3390/s150613348. Licensed under CC BY 4.0

the passive NFC signal and extract the relevant information. NFC technology builds on RFID, which uses an ISO/IEC standard. NFC was approved as an ISO/IEC standard in 2003, and is standardized in ECMA-340 and ISO/IEC 18092. These standards specify the modulation schemes, coding, transfer speeds and frame format of the RF interface of NFC devices, as well as initialization schemes and conditions required for data collision-control during initialization for both passive and active NFC modes. They also define the transport protocol, including protocol activation and data-exchange methods. NFC incorporates a variety of existing standards including ISO/IEC 14443 Type A and Type B.

The possible interaction styles among NFC devices provide three different operating modes, as shown in Figure 1.2 (Coskun et al., 2015). Three types of NFC devices are involved in NFC communication: smartphones, NFC tags, and NFC readers. In reader/writer mode, an active NFC device can read, write or change the stored data in a passive NFC tag. This mode is just like the traditional RFID technology, where a terminal reads the data from the embedded chip on the smart card. The maximum possible data rate in this mode is 106 kbps. In peer-to-peer node, two active devices can exchange small amount of data between them. As both devices are battery-powered, they can establish radio link in between them. They set up a bi-directional, half duplex channel having a maximum data rate of 424 kbps. In card emulation node, the active NFC devices work as a smart card based on ISO/IEC 14443 Type A and Type B. This model is compatible with the pre-existing smart-card industry.

NFC has advantages in IoT application. One of the notable benefits or advantages of NFC revolves around its simplicity and expansive applications. It is easier to set up and deploy than Bluetooth because it does not require pairing or manual configuration. The connection is automatic and takes a fraction of a second. It also uses less power than other types of wireless communication technologies. Another remarkable advantage of NFC is that it supports the widespread application of contactless payment systems. Several companies have implemented payment transactions based on this technology. However, NFC also has disadvantages. It is too expensive for companies to purchase and maintain related machines and other equipment in IoT applications, so small companies could find it difficult to sustain their existing turnover and enhance their profits. Installing the hardware and software and hiring technicians to maintain the same could result in spiraling expenses for the concerned company. A critical limitation or disadvantage of NFC is that it is not as effective and efficient as Bluetooth or Wi-Fi Direct when it comes to data transfer rates. NFC can only send and receive very small packets of data. Its maximum transfer rate is 424 kbps while Bluetooth 2.1 has a transfer rate of 2.1 Mbps. While NFC transactions are undoubtedly more secure than regular credit card payments, this technology is not completely free from risk. Rapid evolution in technology always comes with an equally powerful negative consequence. Mobile phone hacking is now rampant and attackers are coming out with newer methods to gain unauthorized access into users' personal, social security and financial data stored therein. This makes the entire system vulnerable and insecure. The obvious lack of security could discourage both users and companies from warming to this technology in the near future.

NFC offers great and varied promise in services such as payment, ticketing, gaming, crowd sourcing, voting, navigation, and many others. NFC technology enables the integration of services from a wide range of applications into one single smartphone. NFC technology is typically used for payments and marketing applications today. Payment using NFC integrated smart cards offers easier payment compared to conventional multiple step payment process. Top payment services like Visa and MasterCard are offering NFC embedded smart cards to customers. NFC with smart cards can be used for fast payments at grocery shops, parking tickets, adding shopping points, and redeeming coupons with just a single tap of the card. All the major banks around the globe offer smart cards with NFC chips integrated. NFC integrated system can be used in medicine and healthcare activities. NFC offers greater accuracy and convenience in prescribing medicine, easier check-in, payments, checking status of patients, tracking records by embedding NFC tags to patient's charts. NFC integrated devices can be easily paired and configured. Medical professionals can easily check schedules and access medical devices and equipment.

NFC is an emerging technology of the last decade. Even though it remains a comparatively newborn technology, NFC has become an attractive research area for many researchers and practitioners due to its exponential growth and its promising applications and related services. From the technical point of view, some security issues in NFC technology have already been solved and standardization is mostly provided as well. However, there are still unsolved security issues. For example, new protocols/mechanisms on off-line and on-line authentication of NFC tags should be studied. NFC specific alternative key exchange protocols should be proposed to prevent various attacks on RF communication.

BLE

Bluetooth low energy (BLE, Bluetooth 4, Bluetooth Smart) is an innovative technology, developed by the Bluetooth Special Interest Group (SIG), which aims to become the best alternative to the huge number of standard wireless technologies already existing and widespread on the market. Bluetooth wireless technology is an inexpensive short-range radio technology that does not require the use of proprietary cables between devices such as laptops, smartphones, cameras, and printers, with an effective range of 10–100 m. In addition Bluetooth usually communicates at a speed below 1 Mbps, and it uses the specifications of the IEEE 802.15.1 standard. A group of Bluetooth devices sharing a common communication channel is called Piconet. The Piconet can support two to eight devices for data sharing at a time, and the data can be text, pictures, video, and sound. The Bluetooth SIG is composed of more than 1000 companies including Intel, Cisco, HP, Aruba, Intel, Ericsson, IBM, Motorola, and Toshiba.

BLE was first introduced in 2010, and its goal is to extend Bluetooth applications to the applications of power-constrained devices such as wireless sensors, in which the amount of data transmission is small and communication rarely occurs. This differs from conventional Bluetooth applications, such as audio and data streaming, which require a large amount of data transmission and frequent interaction between two communication devices. In addition, device cost is more important for wireless sensor controls than for audio streaming. To address these application requirements, BLE introduces a new radio, which is a derivative of the conventional Bluetooth, and new interfaces. In Bluetooth Classic, there are 79 channels, each with a channel bandwidth of 1 MHz and a raw symbol rate of 1 Msymbol/s. The modulation scheme could be Gaussian frequency shift keying (GFSK), quadrature phase shift keying (4PSK), or 8PSK. For BLE, the modulation scheme is GFSK with raw data rate of 1 Msymbols/s with 2 MHz channel bandwidth, which is double that of Bluetooth Classic.

Zigbee

ZigBee is a low-cost, low data rate, and short distance wireless ad hoc networks standard which contains a set of communication protocols. ZigBee is developed by ZigBee Alliance based on IEEE 802.15.4 reference stack model and mainly operates in two different frequency bands: 2.4 GHz and 868/915 MHz. The original idea of ZigBee-style can be tracked to the end of 1990s, when proposed by the IEEE 802.15 group. After that, IEEE 802.15.4 (TG) group was devoted to the bottom standards. In 2001, ZigBee Alliance was founded by Honeywell and some other companies which aims at creating, evolving, and promoting standards for ZigBee. In 2004, the ZigBee Alliance published the ZigBee 1.0 (a.k.a. ZigBee 2004) standards. Then, the ZigBee 2006, which revised a former version, was published in 2006. In 2007, the alliance published ZigBee PRO standard which contains two sets of advanced commands. In 2009, the standard was more flexible and had remote control capability named ZigBee RF4CE. From 2009, ZigBee adopted IETF's IPv6 standard as the standard of Smart Energy and was committed to forming a globally unified network.

In general, the system architecture of ZigBee is four layers, as shown in Figure 1.3 (Farahani, 2011). As mentioned before, ZigBee is developed at the top of the IEEE 802.15.4 standard. The ZigBee standard is built on the two lower layers: the physical (PHY) layer and the medium access control (MAC) sub-layer which are defined by IEEE 802.15.4, then

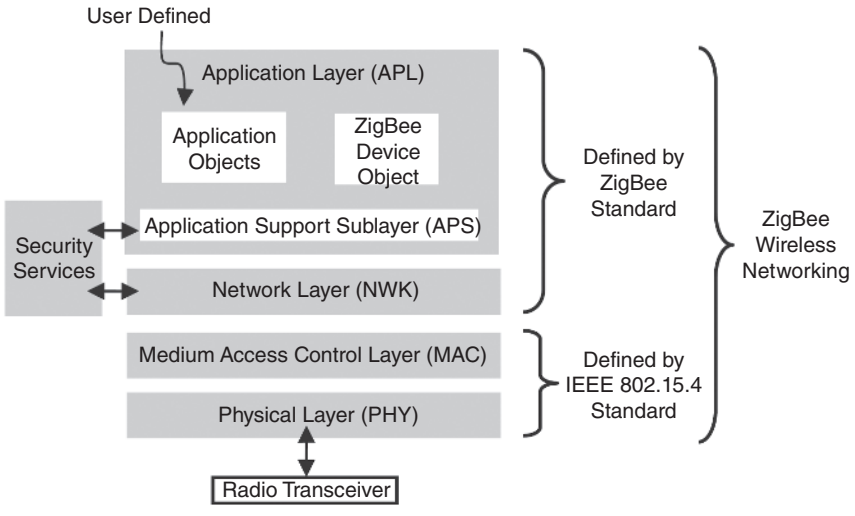

Figure 1.3 Zigbee system architecture. Source: From Shahin Farahani. ZigBee wireless networks and transceivers. Newnes, 2011. © 2011, Newnes.

ZigBee Alliance provides the network (NWK) layer and the framework for the application layer (Alliance, 2012).

PHY: The IEEE 802.15.4 standard defines the PHY layer of ZigBee. The PHY layer is the lowest layer, and defines the interface between the PHY channel and the MAC sub-layer. It also provides a data service and a PHY layer management service. The PHY layer data service directly controls and communicates with the radio transceiver (transmitter and receiver). The PHY layer management service maintains the database which is related to the PHY layer parameters. The protocol stipulates that the PHY layer operate in two separate frequency bands: 2.4 GHz and 868/915 MHz.

MAC: The IEEE 802.15.4 standard defines the MAC layer of ZigBee. The MAC layer provides the interfaces between the PHY layer and the NWK layer and controls access to the radio channel using a CSMA-CA mechanism. The MAC layer is responsible for establishment, maintenance, and termination of wireless links between devices, and it also leads a super-frame structure and transmitting bacon frame into the protocol system.

NWK: The network layer provides interfaces between the MAC layer and the APL layer and is responsible for managing the network and routing. The NWK layer supports three topologies: star, tree, and mesh topologies. Managing the network includes network establishment, end device discovery, join, and departure, and these operations are controlled by the ZigBee coordinator. The ZigBee coordinator is not only responsible for assigning a network address for devices in a network but is also responsible for discovering and maintaining the path in the network due to the terminal devices having no ability for routing. Routing is to choose the path to forward information to the target devices.

APL: The APL layer is the highest protocol layer in the ZigBee standard. The APL layer can be divided into three parts: application support sub-layer (APS), application framework, and ZigBee device object (ZDO). The APL layer is responsible for mapping the variety of

applications to the ZigBee network, and it mainly includes: service discovery, convergence of multiple data stream, and security.

ZigBee has many advantages, and the main characteristics of ZigBee are low data rate, low power consumption, low complexity, high security, and support for a variety of network topologies. However, there still exit some disadvantages. The cost for the end devices is difficult to reduce at present, which makes it is not cheap when deploying a large number of end devices. The communication distance is about 75–100 m, because the communication frequency mainly operates in 2.4 GHz, which is difficult to penetrate through blocks. So obstacles seriously affect the communication distance.

ZigBee is used to provide services such as small area monitors, security, discovery, profiling, and so on for industrial control, household automatic control, and other places where sensor network-based applications are deployed. For example, ZigBee can be used in the building energy consumption monitoring system due to low cost, device sparsity, low energy consumption and self-organized characteristics. The end devices equipped with different sensors are used to monitor the temperature, humidity, voltage, and so on. The end devices can also collect the data from water meters, gas meters and electricity meters. These data, which are gathered from a variety of end devices, will be sent to the upper computer, then the policy will be made by the special system to achieve goals such a energy consumption monitoring, temperature control, and energy-saving operation management.

In summary, ZigBee provides short distance, low complexity, low energy consumption, low data rate, and low cost technology for wireless networks, and it effectively compensates for the vacancies in the low-cost, low-power, and low-rate wireless communication market. ZigBee also has many facets that can be improved, and we believe that if improvements in ZigBee technology don't stop there will be more and more ZigBee-based applications in our lives.

1.2.2.2 Low Data Rate and Wide-area Connectivity Technologies

6LoWPAN

The IoT is an emerging paradigm in which smart objects are seamlessly connected to the internet and can potentially collaborate to achieve common goals such as supporting innovative home automation services. IPv6 over a low-power personal area network (6LoWPAN) is an interesting protocol that supports the implementation of IoT in resource-constrained environments. 6LoWPAN devices are vulnerable to attacks from wireless sensor networks and internet protocols. 6LoWPAN is a protocol definition to enable IPv6 packets to be carried on top of low power wireless networks, specifically IEEE 802.15.4. The concept was born from the idea that internet protocols could and should be applied to even the smallest of devices. The initial goal was to define an adaptation layer – "IP over Foo" to deal with the requirements imposed by IPv6, such as the increased address sizes and the 1280 byte MTU. Its emergence provoked the expansion of LR-WPAN. The bottom layer of 6LowPAN technology espouses PHY and MAC layer standards of IEEE802.15.4, and 6LowPAN desires IPv6 as the networking technology. Its goal market primarily is wireless sensor networks. The 6LowPAN is used because it is based on IPv6. Lo in 6LowPAN stands for low power. IP communications and low power consumption is usually contradictory. WPAN stands for wireless personal area networks. A WPAN is a personal area network for connecting devices around a person. A popular WPAN is Bluetooth. Bluetooth is used to

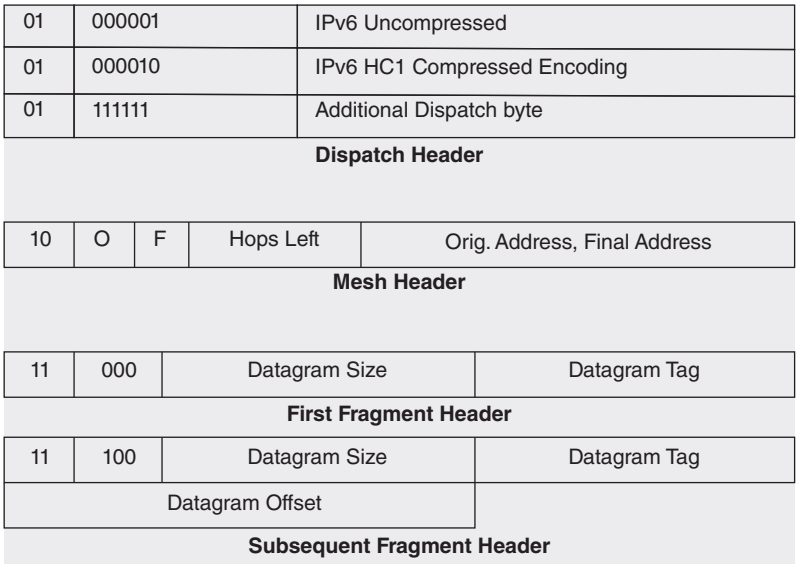

Figure 1.4 6LoWPAN header layout.

interconnect our computer accessories or our audio equipment like Bluetooth headset or hands free kit. 6LoWPAN provides larger scale networks than Bluetooth. 6LoWPAN can create meshed networks with higher distance. By using 868/915 MHz instead of 2400 MHz, the coverage in buildings is much better.

In view of the addresses and security that are claimed in wireless sensor networks, plus the additional expansion of IPv6, initiating IPv6 protocol into embedded equipment has turn out to be an unavoidable propensity. However, the payload length sustained by MAC in IPv6 is greatly larger than one afforded by the 6LowPAN bottom layer. In order to put into practice the seamless connection of the MAC layer and network layer, the 6LowPAN working group recommend adding or toting up an adaptation layer between the MAC layer and the network layer to accomplish the header compression, fragmentation, reassembly, and mesh route forwarding. The reference model of the 6LowPAN Protocol Stack is shown in Figure 1.4.

The fragmentation header includes 4 bytes for the first fragment and 5 bytes for subsequent fragments, as shown in Figure 1.4. It supports a larger fragmentation and payloads than the size of the 802.15.4 frame and also includes fields to specify the size of the original datagram as well as a sequence number for ordering the received packets. The datagram tag field is used to identify all of the fragments of a single original packet. Each 6LowPAN header includes a type identifier and the most common headers are identified with a predefined prefix for each. As shown in Figure 1.4, the dispatch header (1 byte) is used to define the type of header to follow. The dispatch header is identified by the first two bits set to either 00 or 01. In order to provide a means for coexistence with non-6LoWPAN networks, the bit pattern 00 is reserved to identify these non-6LoWPAN frames. The remaining 6 bits indicate if the following field is an uncompressed IPv6 header or an HC1 header defining the IPv6 compressed header. Only 5 of the 64 dispatch header types have thus far been

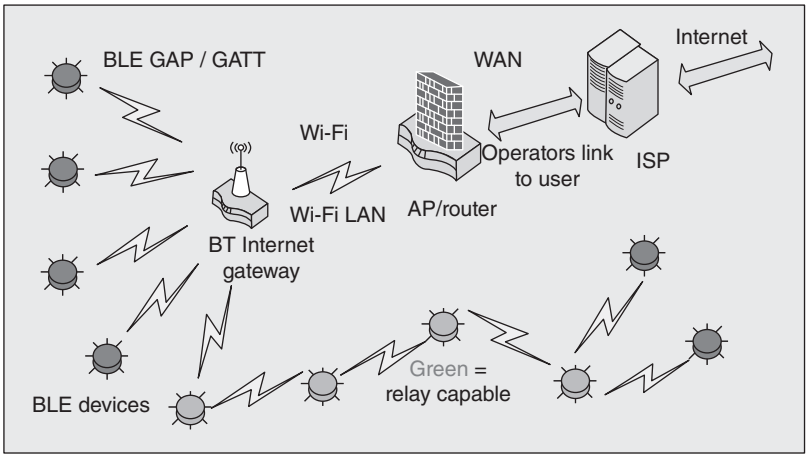

Figure 1.5 A BLE network.

defined. The special value of all ones indicates that the header contains an additional byte to allow for 256 more header types (Mulligan, 2007).

Although 6LoWPAN is not widely known like some other standards, such as RFID and NFC, 6LoWPAN uses IPv6, based on which 6LoWPAN is different from other standards and has obvious advantages. As the world has more and more IoT devices, 6LoWPAN provides advantages for low-power wireless sensor networks and other forms of low-power wireless networks. Due to its flexibility and convenience, 6LowPAN has broad market prospects. 6LowPAN technology is able to support IoT devices, especially in the field of smart city and industrial wireless. 6LowPAN can be used to achieve reorganization of fragments and route optimization. Therefore, when 6LowPAN technology is fully feasible and persistent, it must bring great convenience to people's work and life.

Figure 1.5 presents a network architecture that shows how BLE can be used in IoT applications. Multiples BLE devices are connected by a BT internet gateway or relay nodes. A router could forward the gateway through wireless or wired networks, such as wi-fi and fiber. The upper layers of the network indicates a traditional star network, and the lower layers show how the start network can work in conjunction with a mesh network.

Since IoT applications are broad and diverse, it is certain that the market requires various wireless technologies. However, in the end there will be market winners and losers for a specific application domain. Since Bluetooth is pervasive in smartphones and personal computers, it is gaining ground in home automation applications even though the effort to be a truly low-power technology is still in progress. However, whether Bluetooth Low Energy or Smart, or whatever you call it, will be a dominant technology for applications that only require small amounts of data communications is yet to be seen over time.

LoRa

LoRa (short for long range) is an emerging technology, which operates in a non-licensed band below 1 GHz for long-range communication. LoRaWAN defines the communication protocol and the system architecture, while LoRa defines the physical layer. LoRa Technology offers compelling features for IoT applications including long range, energy efficient

and secure data transmission. The technology can be utilized by public, private or hybrid networks and provides longer communication range than cellular networks. The bandwidth has been established to ensure data rates from 0.3 kbps up to 50 kbps, which is not much compared with IEEE 802.11 but enough for the majority of applications in automation and data collection field, and also ensures maximization of the battery life in the case of mobile or autonomous terminals. The concept is really affordable for IoT applications, especially because of the reduce cost of implementation in long range conditions.

LoRa was invented by a startup in France called Cycleo whose employees are veterans of big semiconductor companies who wanted to build a long range low power communication device. They filed a patent in 2008 titled "Fractional-N Synthesized Chirp Generator" and another in 2013 titled "Low Power Long Range Transmitter". Later this company was acquired by another French company named Semtech that's into manufacturing of analogue and mixed-signal semiconductors. Semtech's LoRa Technology has amassed over 600 known uses cases for smart cities, smart homes and buildings, smart agriculture, smart metering, smart supply chain and logistics, and more, with 97 million devices connected to networks in 100 countries and growing. While Semtech provides the radio chips featuring LoRa technology, the LoRa Alliance, a non-profit association and the fastest growing technology alliance, drives the standardization and global harmonization of LoRaWAN, which is a MAC protocol for LoRa(Augustin et al., 2016). To fully define the LoRaWAN protocol, and to ensure interoperability among devices and networks, the LoRa Alliance develops and maintains documents to define the technical implementation, including MAC layer commands, frame content, classes, data rates, security, and flexible network frequency management, and so on.

A LoRa server architecture consists of end nodes, a LoRa gateway, a LoRa network server, and a LoRa application server, as shown in Figure 1.6. LoRa end nodes are the sensors or application where sensing and control takes place. These nodes are often placed remotely. The nodes are the devices sending data to the LoRa network server. These devices could be

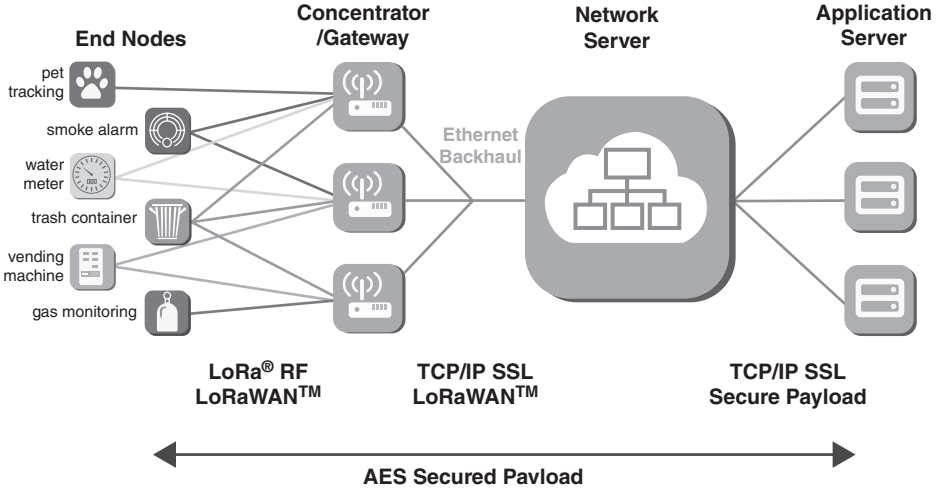

Figure 1.6 LoRa network architecture.

for example sensors measuring air quality, temperature, humidity, location, and so on. The LoRa gateways are different from cellular communication where mobile devices are associated with the serving base stations. The gateways receive data from the devices and typically run an implementation of the packet-forwarder software. This software is responsible for the interface with the LoRa hardware on the gateway. The LoRa server component provides the LoRaWAN network server component, responsible for managing the state of the network. It has knowledge of devices active on the network and is able to handle join-requests when devices want to join the network. When data is received by multiple gateways, LoRa network server will de-duplicate this data and forward it once to the LoRaWAN application server. When an application server needs to send data back to a device, the LoRa network server will keep these items in queue until it is able to send to one of the gateways. LoRa application server provides an API which can be used for integration or when implementing your own application-server. The LoRa application server component implements a LoRaWAN application server compatible with the LoRa server component. It provides a web-interface and APIs for management of users, organizations, applications, gateways, and devices.

Everyday municipal operations are made more efficient with LoRa Technology's long range, low power, secure, and GPS-free geolocation features. By connecting city services such as lighting, parking, waste removal, and more, cities can optimize the use of utilities and personnel to save time and money. LoRa Technology and smart city IoT networking can offer street light solutions that increase energy efficiency and reduce city operating costs. LoRa solutions are easy to implement into existing infrastructure and allow smart monitoring of the grid over a LoRaWAN network. LoRaWAN street light controller is LoRaWAN-alliance network compatible street light control system for street lights. The system provides a unique identity for every light, allows independent control of street lights on a calendar and timer basis, and allows instant manual control of lights from a software control system. LoRa Technology's low-power qualities and ability to penetrate dense building materials make it an ideal platform for IoT-connected smart home and building devices. In addition, the long range capabilities make it possible for LoRa-enabled sensors to track assets that stray from home. Sensors in smart home and building applications can detect danger, optimize utility usage, and improve the safety and convenience of everyday living. LoRa-enabled products can include thermostats, sprinkler controllers, door locks, leakage monitors, and smoke alarms. These devices connect to a building's network and allow consistent, remote monitoring to better conserve energy and predict when maintenance is necessary, saving property managers' money. LoRa Technology has the capacity to function in high density environments, such as in large enterprise buildings or campuses, and can handle thousands of unique messages per day.

LoRa has advantages in IoT applications. LoRa uses industrial, scientific, and medical (ISM) bands 868/915 MHz which is globally available. It has very wide coverage range about 5 km in urban areas and 15 km in suburban areas. It consumes less power and hence batteries will last for a longer duration. Single the LoRa Gateway device is designed to take care of thousands of end devices or nodes, it is easy to deploy due to its simple architecture. LoRa uses the adaptive data rate technique to vary output data rate output of end devices. This helps in maximizing battery life as well as overall capacity of the LoRaWAN network. The physical layer uses a spread spectrum modulation technique derived from chirp spread

spectrum (CSS) technology. This delivers orthogonal transmissions at different data rates. Moreover, it provides processing gain and hence transmitter output power can be reduced with same RF link budget and hence will increase battery life. However, LoRa also has disadvantages. The LoRaWAN network size is limited based on a parameter called the duty cycle. It is defined as the percentage of time during which the channel can be occupied. This parameter arises from the regulation as key limiting factor for traffic served in the LoRaWAN network. LoRaWAN supports limited size data packets, and has longer latency. So it is not an ideal candidate to be used for real-time applications requiring lower latency and bounded jitter requirements.

In summary, the use of LoRa is strongly influenced by the characteristics of the environment in which the technology is implemented. The type of IoT application to be used needs to pay attention to these things. The use of LoRa in open areas such as rural areas has advantages in energy consumption, wide range, and flexibility in network development. However, for applications that require specific requirements such as the amount of data exchanged per specific time period then the network configuration needs to be considered primarily for indoor implementation. The LoRa network cannot transmit large amounts of data for a wider range of territories. LoRa technology is influenced by obstacles such as tall buildings and trees, which leads to an increase in packet loss levels in the zone. The use of GPS in the LoRa module has not been reliable, especially for real-time position tracking software applications. The limitations identified in LoRa technology become an opportunity for future research.

Sigfox

Sigfox was introduced by a French global network operator founded in 2009 and builds wireless networks to connect low-power objects such as IoT sensors and smartwatches, which need to be continuously powered on and emitting small amounts of data (Sigfox, 2018a,b). Sigfox wireless technology is based on LTN (low throughput network). It is a wide area network based technology which supports low data rate communication over larger distances. It is used for M2M and IoT applications which transmit only a few bytes per day. By employing ultra-narrow band in the sub-GHz spectrum, Sigfox efficiently uses the frequency band and has very low noise levels, leading to very low power consumption, high receiver sensitivity, and low cost antenna design. Sigfox developed a simple communications protocol, running in the license-free ISM bands at 868 and 915 MHz. It has very low cost, standard chips, and has a usable range of 5–10 km and a battery life that can support years of low data-rate transmission. Unlike the roll-out of cellular connectivity, where you could start with the areas of greatest use, typically capital cities, the IoT customer base is much more diverse. There are plenty of applications in agriculture and transport that need much wider coverage. Building their own network would have taken too long and cost too much, so they persuaded mobile operators to partner with them and install Sigfox's gateways on their existing towers, providing a fairly rapid coverage. Sigfox has doubled its connected devices from 2019 to 2020, going from around 6.9 million during the first half of 2019, to over 15.4 million at the start of 2020. According to Sigfox, the traffic on Sigfox's networks has increased to 26.5 million messages per day in late March 2020, from 24.6 million at the end of 2019 (https://enterpriseiotinsights.com/20200326/channels/news/sigfox-talks-1b23-and-maturing-of-iot).

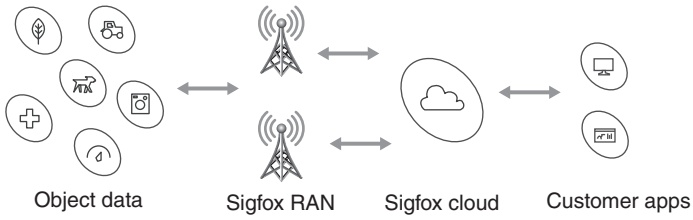

Figure 1.7 Sigfox network architecture.

Figure 1.7 depicts a simple Sigfox network architecture (Sigfox, 2018a,b). The Sigfox network consists of objects (end user devices), a Sigfox gateway or base stations, a Sigfox cloud, and application servers. Sigfox objects are connected with a gateway using star topology. There is a direct secure point to point link between Sigfox gateways and the Sigfox cloud. The cloud interfaces with servers using different protocols such as SNMP, MQTT, HTTP, IPv6, etc. as per end applications. Sigfox offers a software based communication solution, where all the network and computing complexity is managed in the cloud, rather than on the devices. All that together, devices connected through the Sigfox network only use the network when they are actually required to transmit data; in this procedure, much of the power consumption is reduced.

Sigfox has advantages in IoT applications. Sigfox has designed its technology and network to meet the requirements of mass IoT applications, a long device battery life-cycle, low device cost, a low connectivity fee, high network capacity, and long range. A device is not attached to a specific base station. Its broadcast messages are received by any base station in the range, and there is no need for message acknowledgement. UNB intrinsic ruggedness coupled with spatial diversity of the base stations offer great anti-jamming capabilities. UNB is extremely robust in an environment with spread spectrum signals. Low bit rate and simple radio modulation enable a 163.3 dB budget link for long range communications. Sigfox has tailored a lightweight protocol to handle small messages. Less data to send means less energy consumption, hence longer battery life. With its simple approach to connectivity, Sigfox provides extremely price-competitive connectivity subscriptions, and even more importantly, enables extremely simple and cost-efficient silicon modules. Sigfox is compatible with Bluetooth, GPS 2G/3G/4G and wi-fi. By combining other connectivity solutions with Sigfox, business cases and user experience can be drastically improved. However, Sigfox also has disadvantages. The narrow band spectrum emitted by a single Sigfox end device causes strong interference and collision to nearby existing wideband systems. More such sigfox devices will further enhance the interference. Sigfox supports one-way communication without acknowledgment. This necessitates multiple transmissions if the server does not receive data without errors. Due to the multiple transmissions, power consumption will increase which depends on number of re-transmissions. Due to low data rate support, it cannot be used for high data rate applications.

Nowadays, pallet tracking to determine the location of and goods condition are highly desirable in logistics. In this application, the most requirements are low cost sensors and long battery lifetime for asset tracking and status monitoring. In this case, Sigfox is a good solution. Logistics companies can have their own network so they have a guaranteed coverage in their facilities. Low cost Sigfox devices could be easily deployed on vehicles. Sigfox

public base stations can be then used when vehicles are outside of the facilities or when goods arrive at customer locations. In the retail and hospitality industries, keeping guests satisfied and customers engaged is your number one priority. Now, the IoT is here to help. Sigfox-enabled IoT solutions for retail and hospitality change the game by keeping you connected to all aspects of your retail location, hotel, or restaurant powered by Sigfox's network dedicated exclusively to the IoT; the latest IoT solutions improve upon earlier versions of connectivity technology to provide a cost efficient, user-friendly experience.

In summary, Sigfox is rolling out the first global IoT network to listen to billions of objects broadcasting data, without the need to establish and maintain network connections. This unique approach in the world of wireless connectivity, where there is no signaling overhead, is a compact and optimized protocol. However, in order to support a myriad of devices in IoT, the interference between Sigfox devices and nearby existing wideband systems should be mitigated in further research. Further, new technologies and mechanisms should be investigated to reduce re-transmissions. The Sigfox system works well in a fixed location. There are issues such as interference and frequency inaccuracies in mobility environments, which also present challenges to further research and application.

NB-IoT

NB-IoT is a LPWAN technology based on narrowband radio technology. The technology provides improved indoor coverage, support for a massive number of low throughput devices, low delay sensitivity, ultra-low device cost, low device power consumption, and optimized network architecture. The technology can be deployed by utilizing resource blocks within a normal LTE carrier, or in the unused resource blocks within a LTE carrier's guard-band, or standalone for deployments in a dedicated spectrum. NB-IoT is standardized by the 3rd Generation Partnership Project (3GPP). Its specification was published at Release 13 of 3GPP on June 2016 (3GPP, 2016b). In December 2016, Vodafone, and Huawei deployed NB-IoT into the Spanish Vodafone network and sent the first message conforming to the NB-IoT standard to a device installed in a water meter. NB-IoT now has received strong support from Huawei, Ericsson, and Qualcomm. The objectives of NB-IoT are to ensure a device cost below US$5, uplink latency below 10 s, up to 40 connected devices per household, a device with 164 dB coupling loss, and a ten-year battery life can be reached if the user equipment transmits 200 bytes of data a day on average. NB-IoT has entirely an extensive ecosystem that is available globally. This is primarily due to its support from more than 30 of the world's largest and top class operators. These operators have global communication coverage that serves above 3.4 billion customers and geographically serve over 90% of the IoT market (Huawei, 2016b).

NB-IoT network architecture is shown in Figure 1.8. In order to send data to an application, two optimizations for the cellular IoT (CIoT) in the evolved packet system (EPS) are defined, the user plane CIoT EPS optimization and the control plane CIoT EPS optimization (Schlienz and Raddino, 2016). Both optimizations may be used but are not limited to NB-IoT devices. In the control plane CIoT EPS optimization, data are transferred from the eNB (CIoT RAN) to the MME. From there, they may either be transferred via the serving gateway (SGW) to the packet data network gateway (PGW), or to the service capability exposure function (SCEF), which is only possible for non-IP data packets. From these nodes, they are finally forwarded to the application server (CIoT Services). DL data is transmitted

over the same paths in the reverse direction. In this solution, there is no data radio bearer set up, and data packets are sent on the signaling radio bearer instead. Consequently, this solution is most appropriate for the transmission of infrequent and small data packets. The SCEF is a new node designed especially for machine-type data. It is used for delivery of non-IP data over a control plane and provides an abstract interface for the network services (authentication and authorization, discovery, and access network capabilities). With the user plane CIoT EPS optimization, data is transferred in the same way as the conventional data traffic, i.e. over radio bearers via the SGW and the PGW to the application server. Thus it creates some overhead on building up the connection, however it facilitates a sequence of data packets to be sent. This path supports both IP and non-IP data delivery.

NB-IoT has advantages in IoT applications. As it uses a mobile network it offers better scalability, quality of service, and security compared to unlicensed LPWAN such as LoRa/Sigfox. It offers long battery life due to low power consumption or current consumption. NB-IoT also offers extended coverage compare to GSM/GPRS systems, and co-exists with other legacy cellular systems such as GSM/GPRS/LTE. The NB-IoT compliant devices can be deployed/scheduled within any legacy LTE network. This helps them share capacity as well as other cell resources with the other wireless connected devices. NB-IoT modules are expected to be available at moderate cost. It offers better penetration of structures and better data rates compared to unlicensed band based standards (e.g. LoRaWAN and Sigfox). However, NB-IoT also has disadvantages. It offers lower data rates (about 250 Kbps download and 20 Kbps upload) compared to LTE. The bandwidth is about 200 KHz. Hence it is ideal to use NB-IoT for stationary devices. NB-IoT devices need to connect to an operator network via a licensed spectrum. Network and tower handoffs will be a problem, so NB-IoT is best suited for primarily static assets, like meters and sensors in a fixed location, rather than roaming assets.

The strong growth in the NB-IoT market has motivated many analyst firms to create forecasts showing the expected numbers of connections as well as the revenue potential. The global NB-IoT chipset market is expected to grow from $461million in 2020 to $2484million by 2025 at a compound annual growth rate (CAGR) of 40.0%, according to MarketsandMarkets Research Private Ltd (https://www.marketsandmarkets.com/Market-Reports/narrowband-iot-market-59565925.html). The NB-IoT market is a sub-set of this,

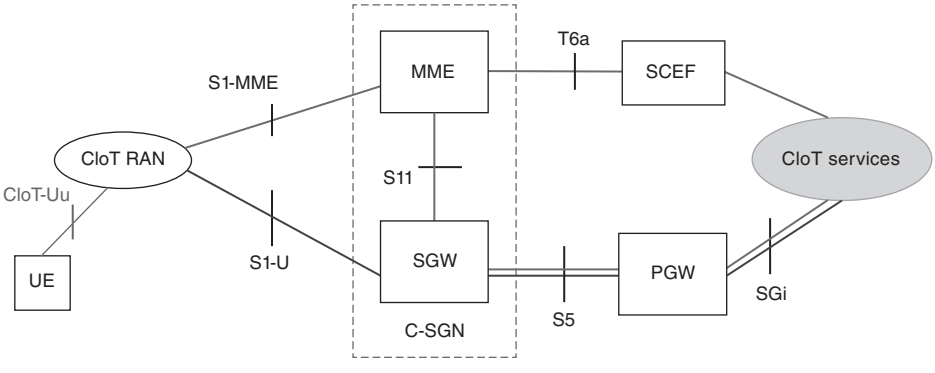

Figure 1.8 NB-IoT network architecture.

and it is important for operators to understand the revenue potential in the countries they operate in. The pet tracking use case is one application that helps the user to keep track of their pet's activities and, most importantly, location at all times. A small lightweight device placed around the neck of the pet embedded with an NB-IOT chip-set helps to send tracking information to the user's device. The NB-IOT device collects and sends location information leveraging GPS and location based services, and this can be done either periodically or in real-time based on the user's preferences. The user can then receive the information with a tracking route that is already integrated with the map. Furthermore, this device is embedded with several forms of alarms that can alert the user when the device battery is running low(Huawei, 2016a). Security has always been a very important aspect of human living; people at all times want to be guaranteed of home safety(Huawei, 2016a). Alarms and event detection will help to rapidly inform that user about a detected home intrusion. NB-IoT system will not only offer intelligent protection from intrusion but will also offer intelligence for detected events that can lead to a fire outbreak like a sudden increase in home temperature or smoke. Alarm and event detectors will make use of sensors placed in devices in ideal locations in the home that constantly communicates with the NB-IoT. This use case will make use of a very low data throughput and battery life of the devices will be ultra-critical.

In summary, NB-IoT is a promising technology for IoT applications. It can connect low-power IoT devices that are placed in weak coverage environments such as apartment basements. This is done by allowing devices to repeat signal transmissions while operating at very low power. Compared to LoRa and Sigfox, NB-IoT relies on the existing cellular infrastructure instead of new ones, thus the investments on a utility-dedicated communication infrastructure and the time required for deployment of applications is reduced. However, it is difficult to implement firmware-over-the-air (FOTA) or file transfers. Some of the design specifications for NB-IoT make it difficult to send larger amounts of data to a device.

1.2.2.3 Emerging IoT Connectivity Technologies and Protocols

MIOTY

Recently, BehrTech, an industrial IoT connectivity provider, has proposed a new IoT technology, called MIOTY, in the burgeoning IoT networking market. MIOTY is another LPWAN solution dedicated to private IoT networks (Behrtech, 2020). MIOTY was originally developed by the Fraunhofer Institute for Integrate Circuits (IIS), and subsequently licensed to BehrTech – is presented as a low-throughput tech for "last mile" industrial communications. As such it goes up against the likes of LoRaWAN, Sigfox, NB-IoT, and LTE-M, variously pushed by their backers as springboards for industrial IoT.

MIOTY is empowered with novel telegram-splitting ultra-narrowband (TS-UNB) to comply with specification from the European Telecommunications Standards Institute (ETSI). MIOTY is based on UNB technology with very narrow signal bandwidth to achieve long distance data communication between thousands of IoT devices and a base station. MIOTY works with standard transceivers. The basic concept of this technology is telegram splitting, which divides a compact telegram transmission into many equally sized radio bursts. TS-UNB, as defined by ETSI, splits the data packets to be transported in the data stream into small sub-packets at the sensor level. These sub-packets are then transmitted over fluctuating frequency and time. An algorithm in the base station permanently scans the

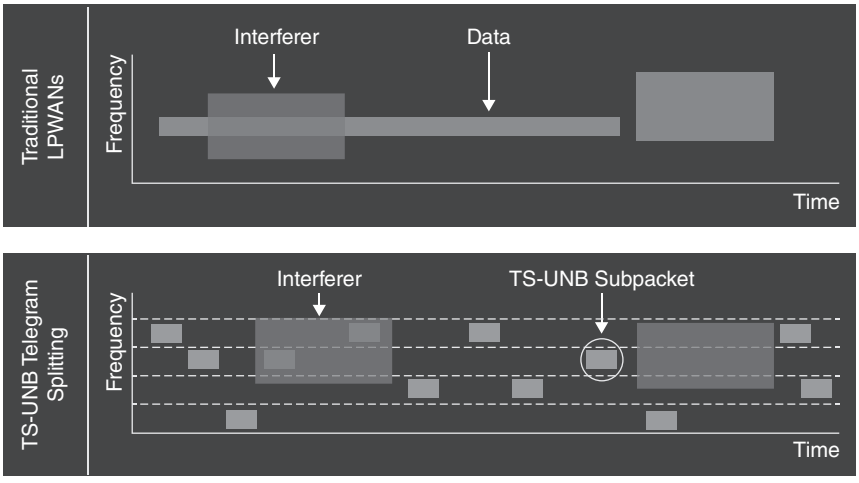

Figure 1.9 TS-UWB telegram splitting.

spectrum for MIOTY sub-packets and reassembles them into a complete message, as shown in Figure 1.9. For multiple access, the radio bursts are distributed over time and frequency. For correct decoding, only 50% of the radio bursts need to be collision free. This reduces the collision probability of telegrams and increases the tolerance against interference.

IoTivity

IoTivity is an open source framework that implements the Open Connectivity Foundation (OCF) standards providing easy and secure communications for IoT devices (Iotivity, 2020). The main goal of IoTivity is to provide seamless device-to-device connectivity regardless of the kind of operating system or communication protocol to satisfy various requirements of IoT. IoTivity is distributed with Apache license 2.0, thus anyone can use it, but revealing source codes based on it is not mandatory. IoTivity is available on multiple platforms and supports a variety of connectivity technologies, including wi-fi, ethernet, BLE, NFC and so on. It works on various OS, such as Linux, Android, Arduino, Tizen, and so on.

The IoTivity framework operates as middleware across all operating systems and connectivity platforms and has some essential building blocks. As shown in Figure 1.10, the discovery block supports multiple mechanisms for discovering devices and resources in proximity and remotely. Data transmission block supports information exchange and control based on a messaging and streaming model. Data management block supports the collection, storage and analysis of data from various resources. The CRUDN (create, read, update, delete, notify) block supports a simple request/response mechanism with create, retrieve, update, delete and notify commands. The common resource model block defines real world entities as data models and resources. Device management block supports configuration, provisioning, and diagnostics of devices. The messaging block of IoTivity is based on resource-based RESTful architecture model. Thus it presents everything (sensors or devices) as resources and uses the CRUDN model to manipulate resources by using IETF CoAP. The ID & addressing block supports OCF IDs and addressing for OCF entities, such as devices, clients, servers, and resources.

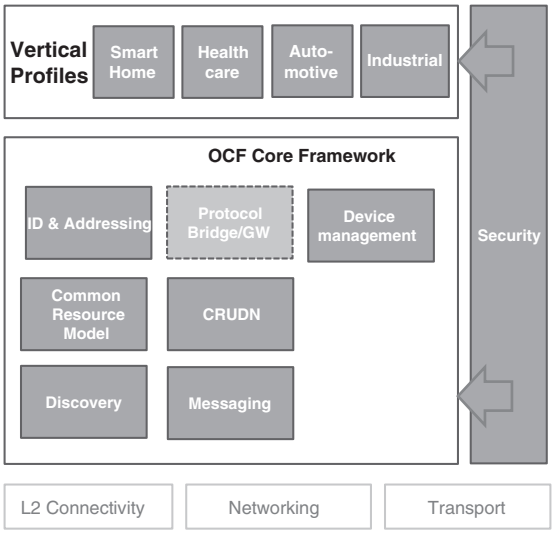

Figure 1.10 OCF core framework.

1.3 Intelligent IoT Technologies

Since IoT was proposed in 1999, its connotation has been in continuous development and expansion (Zhong et al., 2015). At the same time, the scale of devices has also increased at an unprecedented rate. According to the data released by "Statista", the total installed base of IoT connected devices is projected to reach 75.44 billion worldwide by 2025, a five-fold increase in ten years. Details are shown in Figure 1.11. Such a large number of IoT devices undoubtedly put forward higher requirements for the existing IoT (Datta and Sharma, 2017). In order to emphasize the level of intelligent IoT application, this

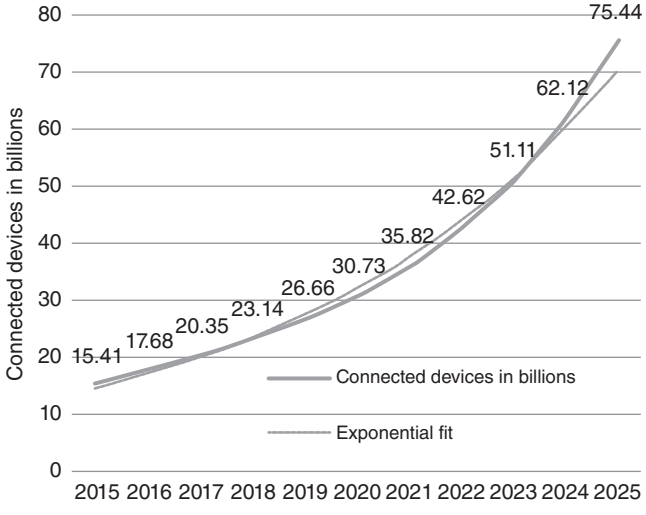

Figure 1.11 The number of connected devices worldwide 2015–2025.

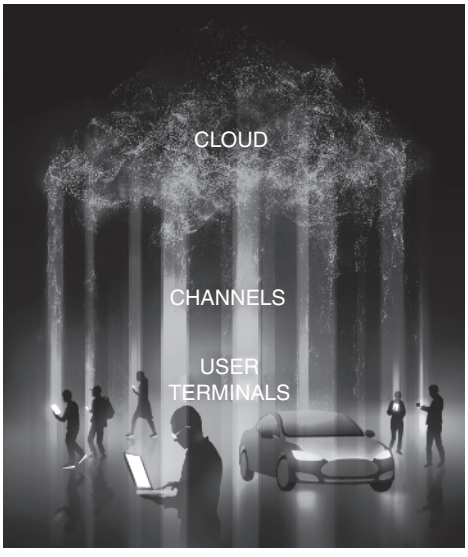

Figure 1.12 A traditional cloud-based IoT architecture.

chapter introduces an intelligent system architecture that can better interpret the meaning and features of the current IoT.

With the rapid adaptation of modern smart technologies, IoT has gained much attention from the industry and the IT community in terms of networking and communication aspects. The number of connected devices to the internet will be huge in number. Traditional architectures and network protocols for IoT devices are not designed to support a high level of scalability, high amount of traffic and mobility together with typical cloud-based applications, such as environmental monitoring and public safety surveillance. In traditional cloud-based solutions, as shown in Figure 1.12, cloud servers are in charge of providing computation, algorithm, and data storage services for IoT users. Based on the services, IoT can provide various productions, services, and platforms for terminal users. However, due to a centralized server, traditional architectures have many issues such as high latency and low efficiency. Furthermore, it's difficult to manage these devices, generating an impressive amount of data as a whole, without having elasticity and flexibility inherently defined in the network. Thus, they are inefficient and have limitations to satisfy new requirements, such as medical monitoring devices, smart grids, transportation systems, and industrial and automation sectors.

Due to such a voluminous number of devices and new requirements, existing network architectures are no longer able to accommodate IoT devices. As users' requirements become more abstract, complex and uncertain, the cloud-based solutions can no longer meet the requirements of IoT users in various aspects, such as latency and computing efficiency. Thus, a generic and flexible multi-tier intelligent IoT architecture distributed computation becomes a potential solution, which is shown in Figure 1.13. In the IoT architecture, IoT applications are increasingly intelligent due to more meaningful data, distributed powerful processors and sophisticated algorithms. Typical IoT applications are also shifting from simple data sensing, collection and representation tasks towards complex information extraction and analysis. However, the applications usually follow rules and principles set by a specific industrial domain. Computing resources integrated

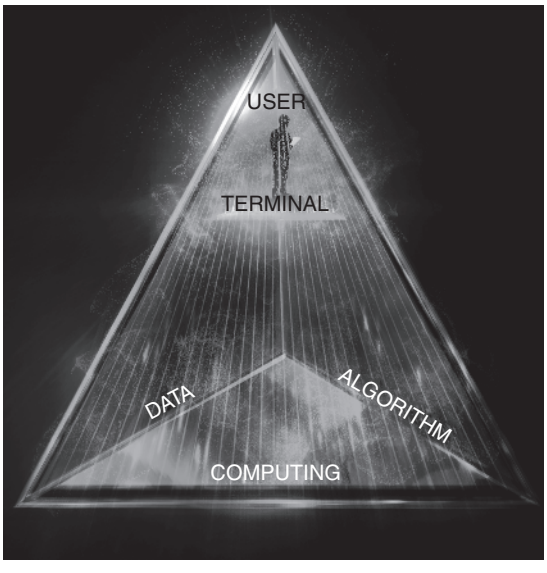

Figure 1.13 A generic and flexible multi-tier user-centered IoT network architecture.

with environment cognition, big data and AI technologies, could be used to develop a user-centric approach in which different IoT services are autonomously customized according to specific applications and user preferences. Furthermore, the intelligent IoT architecture has not been well studied. How to find a scalable, flexible, interoperable, lightweight, energy-aware, and secure network architecture will be a challenge for researchers.

1.3.1 Data Collection Technologies

Section 1.2 mainly reviews the traditional IoT connectivity technologies and related protocols in detail. Due to the massive data exchanged between a large number of connected devices forming the IoT, the need to provide extremely high capacity, data rate and connectivity increase. Thus, 5G wireless networks are considered as a key driver for IoT (Alsulami and Akkari, 2018). In 2015, the International Telecommunication Union (ITU) released the 5G architecture and overall goals, defining three application scenarios for enhanced Mobile Broadband (eMBB), ultra-high reliability and low latency (uRLLC), and mass machine type communication (mMTC), as well as eight key performance indicators such as peak rate, traffic density, and so on, as is shown in Figure 1.14 (3GPP, 2014). Compared to 4G, 5G will offer at least 10 times the peak rate of 4G, transmission delays in milliseconds and connectivity of millions of meters per square kilometer.The initial commercial deployments of NR are already under way during 2019, focusing on eMBB using the Release 15 version of the 3GPP specifications ("Rel-15"). The basis for uRLLC is inherent in the Rel-15 version of the 5G system, especially in respect of support for low latency. For the mMTC component, NR is complemented by the machine-type communications technologies known as LTE-M and NB-IoT already developed by 3GPP in Rel-13, which provide unrivaled low-power wide-area performance covering a wide range of data rates and deployment scenarios(Ghosh et al., 2019). In addition to that formal process, work has progressed on around 25 Release 16 studies, on a variety of topics:

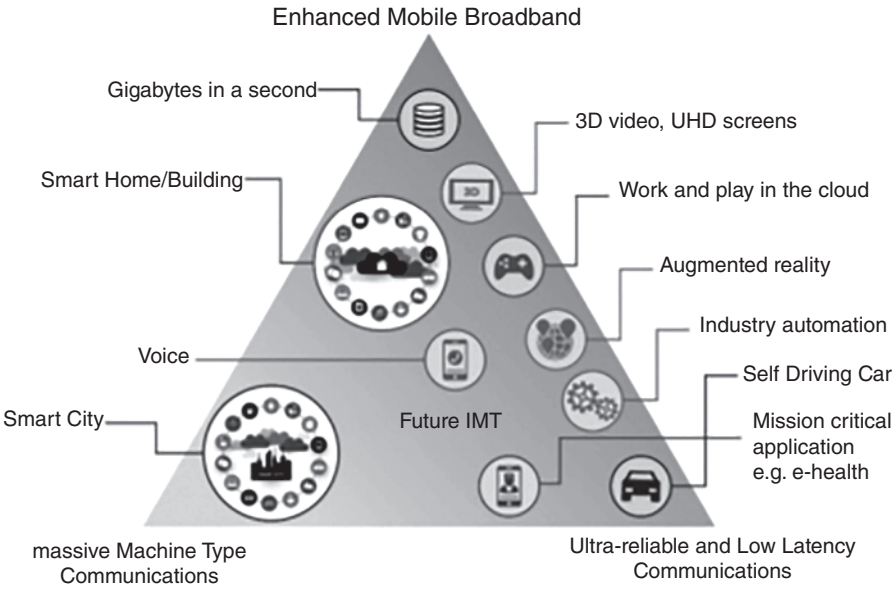

Figure 1.14 Application scenarios of intelligent IoT.

multimedia priority services, vehicle-to-everything (V2X) application layer services, 5G satellite access, local area network support in 5G, wireless and wireline convergence for 5G, terminal positioning and location, communications in vertical domains and network automation, and novel radio techniques. Further items being studied include security, codecs and streaming services, local area network interworking, network slicing and the IoT. 3GPP Release-16 Stage 3 was frozen in June 2020. The R16 standard is deployed for two other scenarios, namely URLLC and mMTC.

The technology of 5G has promoted the development of intelligent IoT. The following is a brief introduction of wireless basic technology and network technology about 5G.

1.3.1.1 mmWave

According to the protocol of 3GPP, 5G networks mainly use two frequencies: FR1 and FR2 bands. The frequency range of band FR1 is 450MHz to 6GHz, also known as the sub-6 GHz band. The frequency range of band FR2 is 24.25–52.6 GHz, often referred to as millimetre wave (mmWave) (Hong et al., 2017). The industry is very familiar with the band below 6 GHz, which is where the 4G LTE network runs. mmWave is relatively unknown, but in the process of 5G network construction, the advancement of mmWave technology will be the key. According to Shannon's formula, we can improve the spectral efficiency or increase the bandwidth to increase the rate (Agrawal and Sharma, 2016).

mmWave is known to have large bandwidths and high rates.The 4G LTE cellular system based on the sub 6GHz band has a maximum bandwidth of 100 MHz and a data rate of less than 1 Gbps. In the mmWave band, the maximum bandwidth available is 400 MHz, with data rates of 10 Gbps or more. In the 5G intelligent IoT era, such bandwidth performance can meet the needs of users for specific scenarios (Khurpade et al., 2018).

1.3.1.2 Massive MIMO

As the frequency used in mobile communication increases, the path loss also increases.However, if the size of the antenna is fixed, such as half wavelength or quarter wavelength, then the increase in carrier frequency means that the antenna is smaller. That means we can cram more and more high-frequency antennas into the same space. Based on this fact, we can compensate for the high frequency path loss by increasing the number of antennas without increasing the size of the antenna array. On the other hand, in the ideal propagation model, when the transmitting power at the transmitting end is fixed, the receiving power at the receiving end is proportional to the square of the wavelength, the transmitting antenna gain and the receiving antenna gain, and inversely proportional to the square of the distance between the transmitting antenna and the receiving antenna. At the millimeter band, the wavelength of radio waves is on the order of millimeters.The radio waves used in 2G/3G/4G are decimeter or centimeter waves. Because the receiving power is proportional to the square of the wavelength, the signal coverage of millimeter wave is small.

Based on the path loss and coverage issues described above, massive MIMO has been introduced. Massive MIMO is a key technology to improve system capacity and spectrum utilization in 5G. It was first proposed by researchers at Bell Laboratories in the United States, and it was found that when the number of base station antennas in a cell reaches infinity, the negative effects such as additive white Gaussian noise and Rayleigh fading can all be ignored, and the data transmission rate can be greatly improved (Gampala and Reddy, 2018). The beam formation of massive MIMO is different from conventional beam formation. Instead of the beam pointing straight at the terminal, it can point at the terminal from many different directions. The signal pre-processing algorithm can arrange the best route for the beam, and it can also send the data through the reflected path from the obstacle to the specified user under precise coordination.

1.3.1.3 Software Defined Networks

As more enterprises evolve their IoT proof-of-concept projects into live architectures, IoT won't be the only technology migration many of them are tackling, as enterprise networks today are also in the midst of a broader, more multi-faceted transformation.

IoT is coming into play just as enterprises are migrating beyond the hub-and-spoke architectures that have defined their networks for decades. In the traditional hub-and-spoke model, all services are processed in a centralized location, and all connectivity goes through that hub. All enterprise traffic from that hub might get backhauled through one or more MPLS links, but that model reflects a previous hardware-centric enterprise IT era, and doesn't allow flexibility to prioritize particular applications or traffic, to access applications from different locations and device types, or to host and process applications in one or more external clouds.

Multiple converging trends in recent years have begun to require a new network approach: the growth and variety of different devices – not just enterprise desktops, but smartphones, IoT sensors and other devices – connected to the network, the proliferation of more distributed networks and remote telecommuting, the ever-present need to reduce enterprise connectivity and hardware costs, the rise of new network connectivity technology options, like broadband internet access and 4G LTE, and an explosion in applications

hosted in a variety of places, not just in an enterprise workstation or a corporate data center, but in a variety of potential cloud locations.

To address the challenges mentioned above, a new concept, software-defined wide area networking (SD-WAN), has emerged in recent years with the aim of simplifying all of this complexity and to help evolve enterprise networks into more flexible, programmable architectures that can meet the changing expectations of users.

SD-WAN accomplishes this by adding software overlay to the enterprise network that separates network control and management functions from the physical network, similar to what software-defined networking can do in a data center or public carrier network.

By separating the control from management in a variety of devices, network elements, and connectivity circuits that make up the network, an enterprise can create pool of total network capacity from these circuits to use as needed, while enabling visibility throughout the network. The visibility allows network managers, in turn, to dynamically identify the best possible paths for high-priority traffic, to allocate the necessary bandwidth and administer required security policies to ensure the quality and integrity of the most mission-critical services.

SD-WAN may play an important role to play in enterprise and industrial networks where IoT is starting to have a larger presence. While many IoT applications do not yet require large amounts of bandwidth on short notice, SD-WAN-based visibility into multiple enterprise connections and control of entire enterprise capacity pools will be able to dynamically allocate bandwidth for mission-critical IoT applications as they emerge, while also segmenting the most latency-sensitive and security-sensitive applications of the industrial IoT.

In addition, SD-WAN's ability to identify new devices coming onto the networks and allocate bandwidth to remote network users will serve enterprises well as they start to expand their IoT network presence throughout their WANs to branch offices and other distributed locations.

Also, SD-WAN can help enterprises manage network architectures in which the edge is becoming the center of data processing and analytics. SD-WAN will play a critical role in connecting, securing and pushing processing power closer to edge devices. This will increase the performance of IoT platforms by reducing latency for processing at the edge, and moving security processes – intrusion detection/prevention, DNS-layer security, and advanced malware protection – near the IoT devices. One of the original arguments for deploying SD-WAN was that it could help lower network expenses for enterprise by employing capacity pools that can help enterprises reduce their reliance on expensive MPLS links by maximizing use of available capacity from other circuits. As more devices and applications emerge in enterprises amid trends like IoT, however, the case for deploying SD-WAN has evolved to become just as much or more about application performance and security in complex network environments as it is about cost savings, according to Oswal. The technology can reduce the need to backhaul traffic from IoT devices all the way to the enterprise data center, instead, transporting that traffic on dedicated secure segments to edge processors that can filter and analyze much of the IoT device data, while transmitting only refined results to clouds for further analysis. This leads to less transport expense, but also faster, more secure application processing.

With its ability to segment traffic, visualize the best possible route paths, and apply appropriate security and network usage policies to different devices on the network could make

sense for enterprises to have SD-WAN overlays in place before they go much further down their IoT road maps. That might not be something some enterprise managers have thought about as they pursued their IoT strategies, but putting the new software layer in place to simplify control of an existing network architecture could make it much easier to introduce a plethora of new IoT-connected devices to the network. Ultimately, IoT is just one emerging enterprise network architecture of many. It doesn't have a unique relationship with SD-WAN, but like other technologies in the enterprise, it can leverage SD-WAN for cost, performance, efficiency and security benefits.

1.3.1.4 Network Slicing

Network slicing (Trivisonno et al., 2017) is to cut the operator's physical network into a number of virtual networks, making each network adapted to different service needs, such as delay, bandwidth, security, reliability, and so on. Through network slicing, multiple logical networks are segmented on a separate physical network, thus avoiding the construction of a dedicated physical network for each service, which can greatly reduce the cost of deployment. Each network slice is logically isolated from the wireless access network to the core network for a wide variety of applications. Network slicing can be divided into at least three parts: a wireless network slice, a carrier network slice, and a core network slice. The core of network slicing (Khan et al., 2020) is network function virtualization (NFV), which separates the hardware and software parts from the traditional network. The hardware is deployed by a unified server, and the software is assumed by different network functions (NFs), to realize the requirements of a flexible assembly business. The basic technology of NFV is mainly cloud computing and virtualization. Virtualization technology can decompose common computing, storage, network, and other hardware devices into a variety of virtual resources in order to achieve hardware decoupling and realize network functions and dynamic flexible deployment as required. Cloud computing technology can achieve application flexibility and even the matching of resources and business load, which can not only improve the utilization of resources, but also ensure the system response speed. The three application scenarios in the existing 5G network architecture are the network slices, which are shown in Figure 1.15.

Network slicing is a logical concept that is based on reorganization of resources. According to the description in (NGMN, 2016), the network slicing consists of three layers: the service instance layer, the network slice instance layer, and the resource layer. The service instance layer represents the end user services or business services that can be supported. Each service is represented by a service instance. The network slice instance layer includes the network slice instances that can be provided. A network slice instance provides the network features that are required by the service instance. The resource layer provides all virtual or physical resources and network functions that are necessary to create a network slice instance (Zhang, 2019). In the context of a large number of network slices, there is a certain complexity in managing and orchestrating network slices. So far, there is no uniform standard for the management of network slices. At present, we can use the existing NFV MANO framework to manage 5G slices (Foukas et al., 2017). At the same time, the emergence of network slicing has also brought great security challenges, and 3GPP has identified many security risks related to 5G network slicing (3GPP, 2017). For example, because services are deployed on the same physical resource based on virtualization

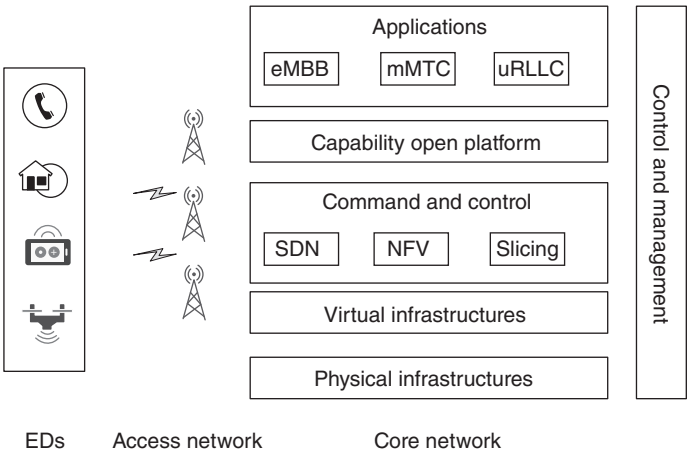

Figure 1.15 Network slices existing in 5G architecture.

technology, if an attacker hoards resources too much on one slice, the performance of other slices may not be guaranteed.

1.3.1.5 Time Sensitive Network

As awareness surrounding IoT standardization continues to grow, more eyes are being drawn to interoperability and network infrastructure solutions, including time-sensitive networking (TSN). TSN is a standard from the IEEE 802 committee and is designed to solve the need to process raw data in a time-critical fashion in addition to reducing latency and increasing robustness. To support new capabilities of IoT-enabled infrastructure, designers, engineers, and end users need to rely on time-synchronized and reliable networking.

TSN provides not only access to a tollway, or an express lane, but along with providing access, the signals along the way are all very tightly coordinated with time. Not only is there the benefit of a priority through the network, but it can actually guarantee end-to-end scheduling, and every light turns green at the right time.

The Avnu Alliance, an industry consortium driving open, standards-based deterministic networking, in addition to advancements made to TSN, is working with member companies to drive this next-generation standard and create an interoperable ecosystem through certification. Members are working within the Alliance to develop the foundational elements needed for industrial applications based on the common elements of AVB/TSN.

In TSN, there are some very interesting and compelling use cases for industry in many applications. However, there is also the possibility of getting onto a new track and using standardized technology, which is the target for most of the innovation in the networking space and leveraging these faster speeds.

TSN promises through standard silicon to converge the previously disparate technologies needed for standard ethernet communication, for deterministic high-speed data transfer, and for high accuracy time synchronization. These developments will create a common foundation that will impact numerous applications and markets ranging from machine control and asset monitoring to test cells and vehicle control. As IIoT adoption continues, increased amounts of data and widely distributed networks will require new standards for sharing and transferring critical information. Just as an ambulance or fire engine receives

priority among other traffic during an emergency, the TSN standard ensures that critical, time-sensitive data is delivered on time over standard network infrastructure.

1.3.1.6 Multi-user Access Control

Effective access control for information collection is one of the major challenges in the development of IoT.

In most applications of the IoT, the data collected by the perception layer of the IoT nodes is usually protected by the secret keys of the nodes. When users want to access the resources, they need to apply to central authority(CA) for the corresponding keys and then decrypt it. Users need to interact with the CA for each access. With the increase of access nodes, users not only need to keep a large number of keys, but also need to communicate with the CA frequently (Feng and Zhu, 2016). This will not only burden users' storage and network communication overhead, but also bring security threats such as DDos attacks and man-in-the-middle attacks. One of the most arduous challenges in the evolution of the IoT is how to reduce communication between users and CA while accessing as many protected node resources as possible.When multiple users access resources protected by nodes in the same perception layer (Liu et al., 2018) they need to obtain the key to access this node. Once a user is attacked by the enemy and the key is invalid, other users cannot access it normally. How to ensure safe and effective access for multiple users is also a problem to consider.

Hierarchical access control schemes are usually used in practice. Through an interaction with the CA, the user can access the information resources of the corresponding level by using the obtained key, and obtain the keys of all levels below the level by using the partial order relationship between the levels to access as many levels of information resources as possible. Since Akl, when Taylor first proposed a hierarchical control scheme based on cryptography, the industry began to put forward different layered control schemes based on different application backgrounds and security requirements, using discrete logarithms to solve the problem and large prime decomposition problem to construct hierarchical access control scheme(Al-Dahhan et al., 2018). This has good expansibility. In addition, the remainder theorem is introduced into the hierarchical access control scheme, which has better storage capacity and a simpler key derivation process.

A single hash function is used to construct a layered key derivation algorithm and a lightweight layered access control scheme is designed, which can not only reduce the requirement of computing power and storage capacity of nodes, but also have dynamic extensibility. However, considering the special environmental requirements of the IoT perception layer, these control schemes cannot be directly applied to the IoT perception layer environment, and the storage and computing costs are too high, so they are not suitable for the resource-limited IoT perception layer environment. Therefore, the Merkle hash tree based hierarchical key acquisition scheme is widely used. This algorithm does not generate the protection keys of intermediate level nodes in the derivation process, which reduces the security risk of the derivation algorithm and has scalability. At this time, the algorithms of multi-user access control are still evolving.

1.3.1.7 Muti-hop Routing Protocol

Multi-hop routing (or multihop routing) is a type of communication in radio networks in which network coverage area is larger than the radio range of single nodes. Therefore, to reach some destination, a node can use other nodes as relays (Pešović et al., 2010).

Since the transceiver is the major source of power consumption in a radio node and long distance transmission requires high power, in some cases, multi-hop routing can be more energy efficient than single-hop routing (Fedor and Collier, 2007).

There are four typical applications of multi-hop routing – wireless sensor networks, wireless mesh networks, mobile ad hoc networks, and smart phone ad hoc networks.

A wireless sensor network (WSN) refers to a group of spatially dispersed and dedicated sensors for monitoring and recording the physical conditions of the environment and organizing the collected data at a central location. WSNs measure environmental conditions like temperature, sound, pollution levels, humidity, wind, and so on.

A wireless mesh network (WMN) is a communications network made up of radio nodes organized in a mesh topology. It is also a form of wireless ad hoc network (Toh, 2001). A mesh refers to rich interconnection among devices or nodes. Wireless mesh networks often consist of mesh clients, mesh routers and gateways. Mobility of nodes is less frequent. If nodes constantly or frequently move, the mesh spends more time updating routes than delivering data. In a wireless mesh network, topology tends to be more static, so that routes computation can converge and delivery of data to their destinations can occur. Hence, this is a low-mobility centralized form of wireless ad hoc network. Also, because it sometimes relies on static nodes to act as gateways, it is not a truly all-wireless ad hoc network.

A wireless ad hoc network (Toh, 1997) (WANET) or mobile ad hoc network (MANET) is a decentralized type of wireless network (Toh, 2001, Murthy and Manoj, 2004, Toh, 1997, Zanjireh and Larijani, 2015). The network is ad hoc because it does not rely on a pre-existing infrastructure, such as routers in wired networks or access points in managed (infrastructure) wireless networks(Zanjireh and Larijani, 2015). Instead, each node participates in routing by forwarding data for other nodes, so the determination of which nodes forward data is made dynamically on the basis of network connectivity and the routing algorithm in use (Zanjireh et al., 2013).

Smartphone ad hoc networks (SPANs, also smart phone ad hoc networks) are wireless ad hoc networks that use smartphones. Once embedded with ad hoc networking technology, a group of smartphones in close proximity can together create an ad hoc network. Smart phone ad hoc networks use the existing hardware (primarily Bluetooth and wi-fi) in commercially available smartphones to create peer-to-peer networks without relying on cellular carrier networks, wireless access points, or traditional network infrastructure. Wi-fi SPANs use the mechanism behind wi-fi ad-hoc mode, which allows phones to talk directly among each other through a transparent neighbor and route discovery mechanism. SPANs differ from traditional hub and spoke networks, such as wi-fi direct, in that they support multi-hop routing (ad hoc routing) and relays and there is no notion of a group leader, so peers can join and leave at will without destroying the network.

1.3.2 Computing Power Network

1.3.2.1 Intelligent IoT Computing Architecture

The data collected by IoT systems is growing exponentially. This will put forward a lot of requirements for the system, including data storage, computing power, and so on. Although the emergence of cloud computing (Armbrust et al., 2010) eases the pressure to some extent, if data is transmitted to the cloud center of remote geographic localization, it will

cause a lot of problems. On the one hand, it could cause a lot of congestion for the network, especially when the network includes a great number of devices and only has limited communication resources; on the other hand, it can lead to a lot of delay. These problems will lead to a bad influence on the applications which need to make timely decisions. There will be a great quantity of computing resource pools distributed in future networks, providing various computing functions for numerous innovative applications in the 5G/AI era. Considering the significant trend of network and computing convergence evolution (NCC) in NET-2030, and the challenges arising from edge computing, it is necessary to research the "computing power network" (CPN) which supports high collaboration between computing and network resources, with optimal user experience. Based on the network-centric idea, collecting network resources, computing resources, storage resources, and algorithm resources information to the network control plane are needed to realize collaborative scheduling. So, offloading computing power to the edge has been proposed (Yu, 2016). A big problem is that the computing resources of the edge are very limited. It cannot meet the computational force requirements of the applications, which need plenty of computing resources. From the above content, we can find that a lot of early work was too one-sided from the initial consideration of only cloud center resources to the latter which focuses too much on edge resources (Guo et al., 2018). They did not consider how to better integrate multi-level collaboration. The authors (Wang et al., 2019b) (Yao et al., 2019) proposed the EdgeFlow system for IoT applications, which is a multi-tier data flow processing system. This system makes full use of the computing and transmission resources of the whole network. However, there are still some application tasks between terminal devices, mobile edge computing servers, and cloud centric servers that cannot achieve maximum resource utilization efficiency. Therefore, it is necessary to build more layers of servers to facilitate the data offloading layer by layer in order to make full use of the resource. In the process of intelligence, the new computing architecture is derived in the end, which is depicted in Figure 1.16. Of course, this involves a lot of problems and challenges. First of all, the total discharge of the tasks in each layer are interlinked. Secondly, the remaining

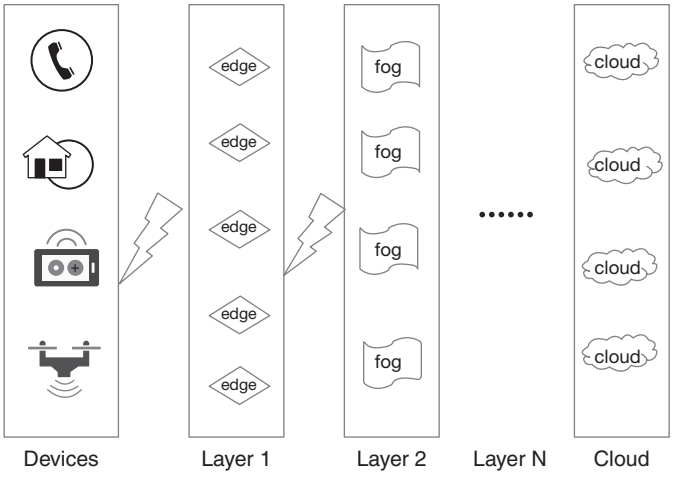

Figure 1.16 The architecture of intelligent IoT multi-tier computing.

resources at each layer also affects the quantity of offloading task. Finally, because of the influence of environmental factors, for example, the volume of resource is in real-time dynamic change, the unloading of tasks and allocation of resources present a great challenge. The heterogeneous mobile edge computing (Het-MEC) was proposed to integrally utilize the computing and transmission resources throughout the entire network, which is a reinforcement learning (RL)-based framework for Het-MEC (Zhang et al., 2020) (Wang et al., 2019c). Here, we explain the multi-tier computing architecture in the internet of intelligent things (IoIT). Different IoT applications have different levels of intelligence and efficiency in processing data. Multi-tier computing, which integrates cloud, fog, and edge computing technologies, will be required in order to deliver future IoT services (Yang, 2019).

1.3.2.2 Edge and Fog Computing

With the advent of a new round of the internet and industrial revolution, the internet will carry the convergence of the heterogeneous network and the dynamic reconfiguration of IoT equipment and personal user devices. To provide the higher performance of internet services, the IoT calculation capability is facing an unprecedented challenge from the actual needs of user services and IoT equipment's resource requirements. 5G (Yu, 2016) is about to be commercialized on a large scale mobile communication technology that will be integrated into the IoT. MEC can decentralize computing and storage services at the edge of the network, near the terminal equipment. Put another way, the MEC is an implementation of the edge computing paradigm that brings cloud computing capabilities to the edge of the mobile network, inside the radio access network (RAN) (He et al., 2018, Mach and Becvar, 2017). MEC nodes are generally located with the radio network controller or with a large base radio station (Dolui and Datta, 2017). Its biggest feature is to sink the core business to the edge of the mobile network, thus enhancing the various types of service quality.

The aforementioned implementations of edge computing share some features. First of all, they have the same aim: to extend cloud capabilities to the edge of the network. Also, they rely upon a decentralized infrastructure, even though, it is accessible through different types of networks (e.g. wireless, mobile, Bluetooth) and are composed of diverse devices. In addition, all edge implementations provide a set of benefits, mainly originated from the proximity to the edge of the networks: low latency, context and location awareness, high scalability and availability, and support to mobility. Undoubtedly, even if these implementations share the same goal and a number of features, they present some differences. They can be deployed in different ways, both in terms of the type of devices and proximity to end users. For instance, the deployment of MEC nodes is linked to the mobile network infrastructure, while mobile cloud computing (MCC) has a wider scope. There are also differences in terms of entities eligible to own these infrastructures. For example, since MEC nodes are bound to the edge of the mobile network infrastructure, only telecommunication companies can provide MEC services, while any entity can deploy an MCC infrastructure.

As a vital part of 5G mobile communication network technology, MEC has a wide range of application scenarios due to its high efficiency and low latency, thus applying it to the industrial internet (Chen et al., 2018b, Sun et al., 2018) also has significant advantages. At present, demand from applications with cross-platform and cross-sector is increasing, and the traditional ethernet has been unable to process the growing data in industry under new requirements of network latency.

According to the characteristics of the IoT, the edge computing platform can be introduced between the core network and the factory 5G wireless base station (Yu, 2016, Feng et al., 2017). The data in the terminal equipment is aggregated to the MEC server after passing through the base station and the internal gateway, then passes to the internet. The MEC server filters the uploaded data, caches part of the data to the edge data center (EDC), and processes and analyzes the data using the idle edge network resources inside the EDC.

Fog computing emerges from the crowd representing the highest evolution of the edge computing principles. In general, the goal of fog computing is to represent a complete architecture that allocates resources horizontally and vertically along the cloud-to-things continuum. Hence, it is not just a trivial extension of the cloud, but a new player in interacting with the cloud and the IoT to help enhance their interactions. However, the research on fog computing is still in its infancy and there are new differences.

Fog computing is often considered as an implementation of edge computing. However, fog computing provides distributed computing, storage, control, and networking capabilities closer to the user (Chiang et al., 2017). Fog computing is not limited to only the edge of the network, but it incorporates the edge computing concept. Fog computing provides a structured intermediate layer that fully bridges the gap between IoT and cloud computing. In fact, fog nodes can be located anywhere between end devices and the cloud; thus, they are not always directly connected to end devices. Moreover, fog computing does not only focus on the "things" side, but it also provides its services to the cloud. The N-tier architecture proposed by the OpenFog Consortium (Martin et al., 2017) is mainly aimed at giving an inner structure to the fog layer of the three-layer architecture, driving the stakeholders when it comes to deploying fog computing in a specific scenario. Indeed, although the deployment of fog software and fog systems is scenario specific, the key features of the fog architecture remain evident in any fog deployment.

In this vision, fog computing is not only an extension of the cloud to the edge of the network, nor a replacement for the cloud itself, rather a new entity working between cloud and the IoT to fully support and improve their interaction, integrating the IoT, edge, and cloud computing.

1.3.3 Intelligent Algorithms

1.3.3.1 Big Data

Big data defines huge, diverse, and fast growing data that requires new technologies to handle. With the rapid growth of data, big data has been brought to the attention of researchers to use it in the most prominent way for decision making in various emerging applications. Big data has always been defined by five most common characteristics: variety (Aftab and Siddiqui, 2018, Li et al., 2013, Batyuk and Voityshyn, 2016, Yadranjiaghdam et al., 2016), volume (Aftab and Siddiqui, 2018, Jain and Kumar, 2015), value (Demchenko et al., 2014, Gürcan and Berigel, 2018), veracity (Gürcan and Berigel, 2018, Benjelloun et al., 2015, Londhe and Rao, 2017), and velocity (Yadranjiaghdam et al., 2016, Kaisler et al., 2013, Yu et al., 2017). Variety indicates that the data is of multiple categories such as raw, structured, semi-structured, and unstructured data from various sources such as websites, social media sites, emails, and documents. The volume indicates very large quantities of generated data.The velocity concept deals with the speed of the data coming from various sources.

Value is the process of extracting valuable information from a huge set of data. It is important as it generates knowledge for people and business. And veracity refers to the accuracy of collected information. Data quality with its privacy is important for correct analysis.

Up to now, big data architecture patterns have emerged. Big data architecture pertains to the basic design and components required for the storage, management, and retrieval of big data in an IT domain. The big data architecture blueprint is categorized as the logical and physical structure and consists of four different layers: big data sources, storage, analysis and utilization. The sources layer includes a server or any data sources such as sensors, social media, and data warehouse. The storage layer collects all the structured data and stores it in the relational database management system or the unstructured data are placed into the Hadoop Distributed File System. Analysis is pivotal for the improvement of the business and the utilization of the outcome to counter complications.

Big data analytics, which is the bridge between big data and the IoT, is a transpiring field. IoT and big data both are two-fold, which can be considered as two sides for the same coin. Analytics of big data is to require to examine the massive sets of data which can contain different types. The social competence of big data and IoT is the emerging key to escalate the decision-making. As we experience the expansion of sensors over every organization/industry, IoT has most eminent attributes to analyze the information about things connected. Analysis of big data in the IoT demands a copious amount of space to store data. The current status of IoT is deficient without the big data. Currently, the IoT is already applied in wide-ranging domains and has been integrated into predicting natural calamities, regulating traffic, adjusting lighting at home, and also in agro-based industries. In the progressive world, the IoT would be much more in demand and have more prominence. This would result in various companies investing more in data centers to store and analyze all the huge amount of data generated from IoTs. Business can multiply their profits by integrating and adapting to personalized marketing, capitalizing on the customers' preference hiking the revenue. Both big data and IoT can be integrated into a larger scale with government and implement smart cities throughout the country to ensure enhanced lifestyle along with reducing time consumption, finances, and exploitation of energy. Agriculture industry could also flourish by evaluating the soil and determining the prerequisites for a better yield and profit.

Big data brings many attractive opportunities and application with a lot of challenges to handle. However, there are still some important challenges of big data to be mentioned. For instance, data does not come from a vacuum. It comes from many sources by underlying activities, examples like web logs, social networks, sensors, scientific research, and experiments that produce huge amount of data (Yu et al., 2017). Raw data generated from a source is too gigantic and everything is not always useful. These collected data have various structures that need to be further processed. So, initially, all data needs to be stored for pre-processing. Apart from these captured data, more data is automatically generated by the system called metadata that defines which type of data will be stored. The available storage is not sufficient enough to store such massive data. One solution is to upload it to the cloud. However, uploading terabytes and zetabytes of data will take a lot of time. Also, due to the rapid nature of data, it is not possible to use the cloud for real-time data processing (Behera et al., 2017). Fortunately, edge computing and fog computing can share a portion of the storage.

In addition, the data generated by users is heterogeneous in nature whereas data analysis algorithms expect homogeneous data for better processing and analysis. Data must be properly structured at the beginning of analysis. Structured data is well organized and manageable. Unstructured data represents all kinds of social network data, documents, and reviews (Behera et al., 2017). Unstructured data is costly to work with and also it is not feasible to convert all unstructured data to structured data. This diversity in data is challenging to handle and process (Katal et al., 2013).

For real-time applications, timeliness must be of top-most priority (Yin and Zhao, 2015). It is difficult to generate a timely response when the volume of data is very huge. Considering an example, it is important to analyze early detection of disease otherwise it is of no help to the patient. To find common patterns, first time is required to scan the whole dataset. And privacy of data is one of the foremost concerns in big data. Preserving the privcacy of a patient's data is essential as there is fear of inappropriate use of personal data which might get revealed when integrating such data from several other sources. Privacy of data is not only a technique but also a sociological problem (Katal et al., 2013). Each day, massive data is generated on social media where a user shares their private information, location, pictures, and so on, which not only reveal the identity of a user but can also be used for criminal activities and fraud.

Now we are in a digital age, which produces huge amounts of data every day. Properly dealing with the shortcomings of big data and making full use of its strengths and integrating innovation with the IoT, will improve the productivity and decision-making ability of society and enterprises.

1.3.3.2 Artificial Intelligence

The IoT is getting smarter. AI is being incorporated – in particular, machine learning – into IoT applications, with capabilities growing, including improving operational efficiency and helping avoid unplanned downtime. The key to such applications is finding insights in data. AI is playing an increasing role in IoT applications and deployments (Holdowsky et al., 2015, Schatsky et al., 2014). There is an apparent shift in the behavior of companies operating in this area. Venture capital investments in IoT start-ups with AI are rising sharply. Companies have made much progress at the intersection of AI and the IoT in recent years. And major vendors of IoT platform software are now offering integrated AI capabilities such as machine learning-based analytics.

AI is playing a starring role in IoT because of its ability to quickly wring insights from data. Machine learning, an AI technology, brings the ability to automatically identify patterns and detect anomalies in the data that smart sensors and devices generate, such as temperature, pressure, humidity, air quality, vibration, and sound. Companies are finding that machine learning can have significant advantages over traditional business intelligence tools for analyzing IoT data, including being able to make operational predictions up to 20 times earlier and with greater accuracy than threshold-based monitoring systems. And other AI technologies such as speech recognition and computer vision can help extract insight from data that used to require human review.

The powerful combination of AI and IoT technology is helping companies avoid unplanned downtime, increase operating efficiency, enable new products and services, and enhance risk management.

1.4 Typical Applications

1.4.1 Environmental Monitoring

Environmental monitoring is an important application area of the IoT. The automatic and intelligent characteristics of the IoT are very suitable for monitoring environmental information. Generally speaking, the structure of the environmental monitoring based on IoT includes the following parts. The perception layer provides the main function to obtain environmental monitoring information, such as temperature, humidity, and illumination, through sensor nodes and other sensing devices. (Lazarescu, 2013) introduces an application of the IoT in birdhouse monitoring. Because environmental monitoring needs to be perceived in a wide geographical range and contains a large amount of information, the devices in this layer need to be formed into an autonomous network through wireless sensor network technology, extract useful information employing collaborative work, and realize resource sharing and communication through access devices with other devices in the internet. The accessing layer transfers information from the sensing layer to the internet through the wireless communication network (such as wired internet network, Zigbee, LPWAN, WLAN network, GSM network, TDSCDMA network), satellite network, and other infrastructures. The network layer integrates the information resources within the network into a large intelligent network that can be interconnected to establish an efficient, reliable, and trusted infrastructure platform for the upper layer of service management and large-scale environmental monitoring applications. The service management layer conducts real-time management and control of the massive amount of information obtained by environmental monitoring within the network through a large central computing platform (such as high-performance parallel computing platform), and provide a good user interface for the upper application. The application layer integrates the functions of the bottom layer of the system and builds the practical application of the industry oriented to environmental monitoring, such as real-time monitoring of ecological environment and natural disasters, trend prediction, early warning, emergency linkage, etc. Through the above parts, environmental monitoring based on the IoT can realize collaborative perception of environmental information, conduct situation analysis, and predict development trends.

1.4.2 Public Safety Surveillance

Public safety surveillance based on the IoT with the characteristics of wide coverage of public security monitoring, multiple monitoring indicators, high continuity requirements, unsuitable environment for manual monitoring, and close correlation between perceived information content and people's lives, employs the technology of the IoT, in particular the technology of a sensor network to construct an information system engineering composed of a perception layer, network layer, and application layer, which mainly includes monitoring to ensure the safety of all kinds of production scenarios, the monitoring of producer safety, the monitoring of the safety of specific items, the monitoring of densely populated places, the monitoring of important equipment and facilities, and information collection of scenes, personnel, and items during emergency treatment in accidents. Public security is the cornerstone of national security and social stability. In order to effectively withstand all

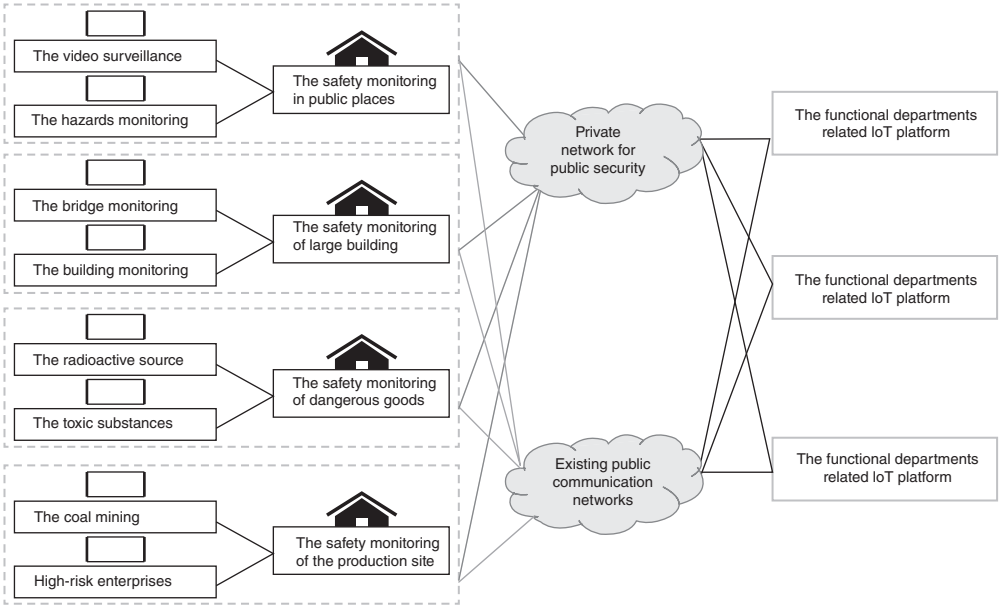

Figure 1.17 The network architecture of public safety surveillance.

kinds of man-made or natural disasters, countries will strengthen public security measures as the focus of government work. The IoT for public safety monitoring provides a new way to solve the problems facing public safety surveillance at present. The establishment of a complete public safety surveillance based on IoT will provide effective prevention mechanism for existing safety problems such as bridge tunnel collapse, hazardous material leakage, etc. The nationwide public safety surveillance based on IoT enables the timely, powerful, and transparent resolution of major safety incidents. Therefore, public safety surveillance based on the IoT should be given priority by the whole of society. The Figure 1.17 describes the network architecture of public safety surveillance based on the IoT, which is similar to the whole architecture of the IoT and consists of three parts: perception layer, network layer and application layer. However, due to the particular needs of public safety surveillance based on the IoT, there are some technical characteristics that other IoT applications do not have, which are summarized as follows.

In the perception layer, the types of perceived information are diverse, and the real-time requirement is high. The monitoring of most information (such as the safety of bridge buildings, monitoring of dangerous goods, etc.) requires high accuracy and is difficult to detect by manual means. Because of the high uncertainty of the information type of potential security hazards, a large number of different types of sensors should be deployed in densely staffed or high-risk production sites for a long time. Higher requirements are put forward for the networking strategy of perception layer, energy management, transmission efficiency, quality of service (QoS), sensor coding, address, frequency, and electromagnetic interference. These problems are also the key to the mature application of public safety surveillance based on the IoT. Because the information perceived by public safety surveillance based on the IoT involves the national key industries and the daily life of the people, once the information is

leaked or improperly used, it may endanger national security, social stability, and people's privacy. Therefore, it is necessary for the information content of public safety surveillance based on IoT to be transmitted through a private network or 4G mobile network after taking security precautions to ensure the security, authenticity, and integrity of the information. It is necessary to establish a proprietary platform for public safety surveillance based on the IoT with different levels in view of the massive amount of data information and the serious harm that hidden dangers to security may bring. The service platform not only has the strong ability of information processing and integration, but also has timely links to relevant functional departments to deal with emergencies in case of public safety emergencies, so as to minimize losses and impact. In addition, the interconnection of public security IoT platforms of different levels is conducive to the maximum allocation of resources according to the hazard level of security incidents, so as to facilitate the timely, effective, and transparent resolution of public security incidents.

In public safety surveillance and environmental monitoring, massive sensor devices, such as for water level, temperature, cameras and microphones, obtain a large amount of data from the environment and transform it into more effective information through multi-level processing and analysis. In this process, in order to protect privacy, the storage, transmission and process of data must be strictly managed. Throughout the system, the transmission of data at each processing stage usually uses encryption technology to ensure the confidentiality of the data. With "smart" becoming the new default on devices, privacy risks are not always clear. Therefore, all IoT devices should adopt basic technologies for privacy protection, such as encrypted data and strong authentication. In terms of storage, we can only store the necessary and important information to protect information privacy. Information, such as video and audio, is transported only in the case of "need-to-know". Anonymization could be used to disguise the identity of the stored information. Sensitive data must be processed in a suitable manner and for the processing aim only. The admission and authentication of the data owner need to be acquired before exposing data information to third parties.

1.4.3 Military Communication

An interesting application scenario that is receiving great attention consists of a collaboration between sensors and mobile agents, typically unmanned air vehicles (UAVs) that are used for retrieving data from the sensor network, to clarify observations and to provide efficient information for mission-critical planning purposes. Such an architecture is illustrated in Figure 1.18, with the main advantage of the UAV is that it provides reach back to a remote command center. The sink is responsible for completing the request from the UAV to obtain information about the observation. Figure 1.18 shows the need for the sensor network to obtain and deliver critical information rapidly and dependably to support the overall mission operation and objectives. To support this, getting to the designated specified region of interest is a critical first step to the overall mission objective. A new routing protocol, called Swarm Intelligent Odour Based Routing (SWOB), had been proposed to solve this critical first step (Ghataoura et al., 2009). SWOB uses network topology and geographic location information to effectively coordinate the routing tasks for information agents to traverse the network to the region of interest. SWOB itself takes its inspiration on

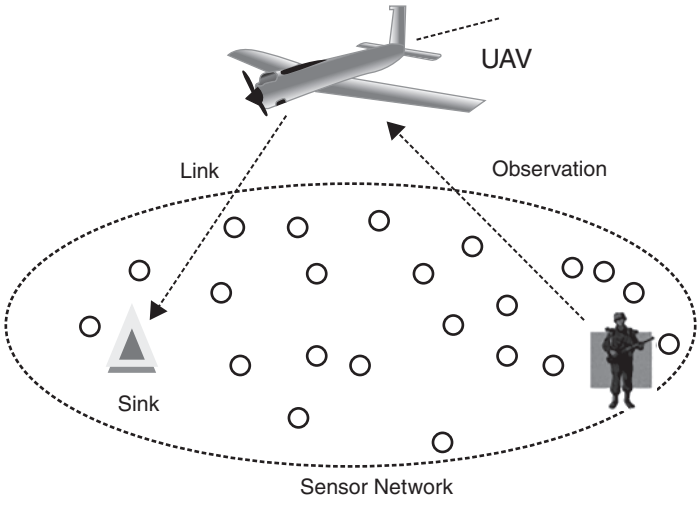

Figure 1.18 Intelligent transportation system scenario overview.

the basic principles and examples provided by social insects in odor localization and tracking. A wide variety of insects use plumes of pheromones (odor) to locate prey, mates, and other sources of particular interest. Insects themselves follow a route employing olfactory sensing to regions of higher pheromone concentration, since this represents a higher order of relevance in finding the required designated odor source. In this study, a virtual Gaussian odor plume is used to conceptually describe the odor dispersion effects found in nature and to establish the level of virtual odor concentration found in a sensor nodes environment, downwind from the odor source (region of interest). Using a virtual Gaussian odor plume model allows information agents to be controlled by an odor plume, with the eventual aim of guiding the designated region of interest. In this case, agents are forwarded in a unicast fashion to nodes that represent higher levels of odor concentration, dictated by the guidance of the virtual odor plume. As a result, the SWOB mechanism has advantages in energy and bandwidth efficiency, and distributed task management and scalability. So that nodes outside the Gaussian plume do not contribute to forwarding tasks and fewer nodes will be competing for bandwidth resource.

However, due to the limited resources of IoT devices in military communication, the existing data security protection method is not fully applicable to high security military communication. Moreover, the highly dynamic environment of the IoT network also makes the military communication more vulnerable and difficult to protect. Therefore, the security goals of confidentiality, authenticity, integrity and availability are still the pursuit of data proposed by the military communication system. Confidentiality means information transmission between objects must be protected from attackers. Access to the system and sensitive information is allowed for legal users only. Integrity is required to ensure data accuracy and completeness and keep it from being tampered with. In the end, to avoid any possible operational interruptions or failures, the availability of the security service must be increased.

1.4.4 Intelligent Manufacturing and Interactive Design

The IoT has been a hyped topic for nearly a decade now. Ever increasing, millions of devices get direct access to the internet, providing a plethora of applications, e.g. smart homes or mobile health management. This trend can also be found in industry where IoT components hardened for these environments have been introduced, called industrial IoT (IIoT) devices, which can be either sensors or actors, as well as mobile equipment such as smartphones, tablets, and smart glasses. Hence, mobile communication has become ubiquitous in smart factories. IIoT devices provide massive data on temperature, pressure, machine states, etc. In comparison to conventional data acquisition in machines, the amount of data will increase significantly and the interaction between machines on the edge as well as between distributed machines and cloud services (Munoz et al., 2016) will rise.

Digitalization, Industry 4.0 or Advanced Manufacturing are programs which are pushing the progress described before. Additionally, they are bringing the flexibility of production sites and systems in the digital era to a new level which has led to new constraints and requirements regarding the communication networks (Chen et al., 2018a). Although the basic concepts have been used for many decades now, production sites and systems are optimized using methods like the Toyota Production System, the Lean concept, and many other techniques. These require a continuous improvement of the whole setup of manufacturers, meaning that machines and components are physically moved around the site to increase the flow of produced parts and products (Ramprasad et al., 1999). Additionally, the demand for individual personalized products is increasing, not only for consumer products, but also for professional products. IIoT components in modern factories on communication networks are neglected and will lead to huge issues for network architecture, network performance engineering, and IT security. This causes flexible requirements on the autonomous configuration of the network and its elements from the component at the edge through the backbone to the source or sink of communication (Ma et al., 2017). Network slices are often used in the backbone parts of a network to allow for a differentiation of the various types of communication and data streams, especially in the context of 5G technology (Rost et al., 2017). This concept solely is neither able to cope with physical flexibility at the edge, nor with the demand of production systems that require end-to-end guarantees (Chien et al., 2019), which have been known in the past for performance engineering based on integrated services. These concepts focus on performance, but not on flexible architecture or IT security which are also required for flexible production systems beginning at the edge (Vilalta et al., 2016). One solution to overcome these challenges are software designed networks (SDNs), allowing for an agile and flexible network configuration. Virtual network functions (VNFs) are dividing the issue into smaller and more manageable elements. The network service, assembling the services of multiple VNFs, enables the machine park operator to connect existing machines to the cloud-based services such as data analytics. Subsequently, the data is processed to provide additional knowledge and services. Data analytics is supporting machine park operators to identify maintenance intervals, incidents with machines or potential increase in performance. SDNs will offer the flexibility for production systems as they are required (Choo et al., 2018).

Data analytics can be used to support machine park operators, but for data analytics machine data is required. Therefore, in this section the focus is on machine data acquisition

in factories. Machines generate constantly data such as operational data, machine data, and process data (O/M/P data). Often, most of the data is only used within the machine, but due to topics such as big data and data analytics, the interest in using these data and further data is growing. As a result, the requirements to factory networks increase dramatically.The machine is controlled by a programmable logic controller (PLC) which reads sensor input data ($S_1 \ldots S_n$) and generates output data for actuators ($A_1 \ldots A_n$) across analogue and digital input and output (I/O) modules. The machine's MPC provides data directly via standardized high-level interfaces for data acquisition by central computers or manufacturing execution systems (MESs).

Furthermore, additional IIoT sensors are becoming increasingly important; for measuring specific temperatures and pressures inside a machine, or for considering ambient conditions such as temperature and humidity. With these retrofit procedures, existing older machines can be integrated into novel data analysis systems as well. Upcoming 5G technology for mobile radio edge communication will pave the way for this. These general conditions indicate that flexible SDN/NFV-based network components are useful for the digitalization of factories.

In addition, network services for intelligent manufacturing must fulfill manifold requirements and use cases as flexible and agile networks will become mandatory in the future.

1.4.5 Autonomous Driving and Vehicular Networks

Autonomous driving includes video cameras, radar sensors(ultrasonic radar, millimeter-wave radar) to sense the traffic or conditions around them and to navigate the road by integrating GPS (global positioning system), IMU (inertial measurement unit), and other information. Perception, planning, and control are the three core functions of existing autonomous driving. The perception layer obtains sensor and other shared communication information as input and transmits it to the planning layer. The planning layer will receive feedback information from the control layer in addition to the perception layer information, and the control layer will realize specific vehicle control.

In order to realize full-scene automatic driving, in addition to dealing with the basic driving environment, the autonomous vehicles also need to overcome the limitations of a rainy day, fog, night, and other harsh environments. At this time, the sensor of the autonomous vehicles alone is far from enough to meet the requirements.This requires the cars have the ability to "telepathically" communicate with participants in traffic scenarios such as roads, traffic signs, and other vehicles over long distances, and allows the car to perceive the complexity of the road in advance, from the distance beyond its line of sight. At this point, network and communication technology can realize autonomous driving more reliably and efficiently by obtaining real-time information shared by a large number of vehicles.

First, the intra-vehicle interconnection communication includes wired and wireless connections, which is further divided into a point-to-point communication mode and data bus communication mode. The wired connection technologies of intra-vehicle interconnection communication include CAN, LIN, FlexRay, MOST (media oriented system transport), idb-1394 (intelligent transport system data bus), D2B (digital data bus), LVDS (low differential signaling), ethernet, PLC (power-line communication). The wireless connection technologies of intra-vehicle interconnection communication include Bluetooth 5.0, ZigBee, UWB (ultra wideband), wireless fidelity, etc(Wang et al., 2019a).

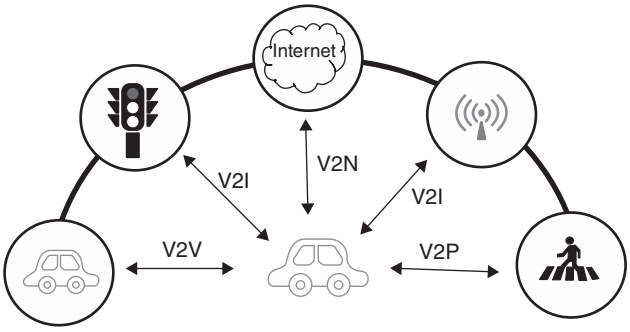

Figure 1.19 Description of VANET for autonomous vehicles.

Secondly, V2X technology is used for inter-vehicle communication (Dietzel et al., 2014). VANET (vehicular ad-hoc network) is the application of traditional MANET (mobile ad-hoc network) on a trafficked road. V2X technologies have V2V (vehicle-to-vehicle), V2I (vehicle-to-infrastructure), V2P (vehicle-to-pedestrian) and V2N (vehicle-to-network), which is shown in Figure 1.19. VANET adopts ICN (information-centric networking) architecture, which can meet the requirements of high scalability and low delay of autonomous driving. It can address data directly by changing the addressing scheme, rather than using the location of the data. In addition, the clustering can improve the scalability and reliability of VANET to meet the requirements of the autonomous vehicle networks (Cooper et al., 2017). The potential inter-vehicle communication technologies in autonomous driving include low power technologies (Bluetooth, ZigBee), IEEE 802.11 family technologies [wifi, DSRC (dedicated short range communications (Kenney, 2011))], base station driven technologies [WiMAX (worldwide interoperability for microwave access), LTE-V (long term evolution for vehicles)] (Chen et al., 2016) and some auxiliary technologies [HetVNET (heterogeneous vehicle network), SDN].

Current Cellular Vehicle-to-everything (C-V2X) technology, which is based on cellular communications, allows cars to have this capability. For example, communication with traffic lights can let the car know the status of traffic lights in advance, and thus it can slow down in advance. By communicating with other vehicles, we can inform other vehicles of emergency braking, lane changes, and turning status in time, so that other vehicles will have enough time to predict and deal with it. V2X communication technology can not only enable vehicle-to-vehicle communication, but also enable the big data platform in the cloud to communicate with the vehicle. In addition to enabling the vehicle to enjoy a variety of colorful network services, it can also enable the cloud platform to conduct unified scheduling and integration of all traffic participants, so as to achieve truly intelligent traffic without congestion.

1.5 Requirements and Challenges for Intelligent IoT Services

1.5.1 A Generic and Flexible Multi-tier Intelligence IoT Architecture

Sensing, communication, computing and networking technologies continue to generate more and more data, and this trend is set to continue. Future IoT devices could,

in particular, be widely deployed for tasks such as environmental monitoring, city management, and medicine and healthcare, requiring data processing, information extraction, and real-time decision making. Cloud computing alone cannot support such ubiquitous deployments and applications because of infrastructure shortcomings such as limited communication bandwidth, intermittent network connectivity, and strict delay constraints.

To address this challenge, and ensure timely data processing and flexible services, multi-tier computing resources are required, which can be deployed and shared along the continuum from the cloud to things. Cloud computing technologies are usually centralized and used for global tasks. Multi-tier computing involves collaborations between cloud computing and fog computing, edge computing and sea computing technologies, which have been developed for regional, local and device levels, respectively (Figure 1.1). The integration of these different computing resources is vital for the development of intelligent IoT services.

Thus, it is essential to have effective communication and collaboration mechanisms across different levels and units. Similarly, interaction and collaboration between cloud, fog, edge and sea computing are vital in order to create an intelligent collaborative service architecture. As a result, this architecture actively connects the shared computing, communication and storage resources of all the nodes in the IoT network, and fully utilizes their capabilities at different locations and levels, in order to provide intelligent, timely and efficient services according to user requirements. Since most applications and their data do not require superior computing power, this architecture can significantly improve service quality and user experience while saving time, resources and costs.

1.5.2 Lightweight Data Privacy Management in IoT Networks

The IoT is composed of physical objects embedded with electronics, software, and sensors, which allows objects to be sensed and controlled remotely across the existing network infrastructure, and facilitates direct integration between the physical world and computer communication networks. The advancement and wide deployment of the IoT have revolutionized our lifestyle greatly by providing the most convenience and flexibility in our various daily applications. The typical applications of IoT include smart grid, healthcare, and smart city. The IoT has been widely applied in various applications such as environment monitoring, energy management, medical healthcare systems, building automation, and transportation. With the rapid deployment of IoT technologies and the variety of IoT applications, there is a need for new tools to ensure individual privacy requirements when collecting and using personal data (Dorri et al., 2017).

Unfortunately, due to the constraints of communication and computation resource of IoT devices, highly complex computation is delivered to the energy abundant cloud for considerably enhanced efficiency. However, due to the wide-area data transmission and resource constraints of the devices, IoT security and privacy remain a major challenge, and new efficient privacy-preserving solutions for intelligent IoT applications are required.

In recent years, fog computing-enhanced IoT has recently received considerable attention, as the fog devices deployed at the network edge can not only provide low latency and location awareness but also improved real-time and quality of services in IoT application

scenarios (Lu et al., 2017, Mukherjee et al., 2017). However, existing security and privacy measurements for cloud-based IoT cannot be directly applied to the fog computing-enhanced IoT due to its features, such as mobility, heterogeneity, and large-scale geo-distribution. For example, all devices in fog networks have a certain level of reliance on one another. Authentication plays a major role in establishing an initial set of relations between IoT devices and fog nodes in the network. However, this is not sufficient as devices can always malfunction or are also susceptible to malicious attacks. In such a scenario, trust plays a major role in fostering relations based on previous interactions. Trust should play a two-way role in a fog network. That is, the fog nodes that offer services to IoT devices should be able to validate whether the devices requesting services are genuine. On the other hand, the IoT devices that send data and other valued processing requests should be able to verify whether the intended fog nodes are indeed secure. This requires a robust trust model in place to ensure reliability and security in the fog network.

1.5.3 Cross-domain Resource Management for Intelligent IoT Services

With the wide adoption of the IoT across the world, the IoT devices are facing more and more intensive computation task nowadays. However, with limited battery lifetime computation, bandwidth, and memory resources, the IoT devices are usually limited by their computing capability, latency, and energy, and IoT devices such as sensors, cameras and wearable devices have a computation bottleneck to limit the support for advanced applications such as real-time image processing and low latency online gaming. Fog and edge computing provide new opportunities for developments of IoT since fog and edge computing servers which are close to devices can provide more powerful computing resources. The IoT devices can offload the intensive computing tasks to the servers, while saving their computing resources and reducing energy consumption (Cui et al., 2019). However, the benefits come at the cost of higher latency, mainly due to additional transmission time, and it may be unacceptable for many IoT applications. One critical problem in the computation offloading is the selection of the fog and edge device from all the potential radio device candidates within the radio coverage area. This is further complicated by the determination of offloading rate, i.e. the number of computation tasks to offload to the edge device. An IoT device often requires a longer period to transmit the offloading data and receive the computation result compared with the local computation within the IoT device. This is further complicated by the chosen edge device carrying out heavy workloads and experiencing degraded radio channel fading and interference. It is, therefore, challenging for an IoT device to optimize the offloading policy within the dynamic network with time-variant radio link transmission rates, especially with an unknown amount of the renewable energy within a given time duration. Thus, it is a challenge to find a trade-off between various cross-domain resources, such as computing power, energy consumption and latency. IoT networks require effective and efficient resource management solutions.

1.5.4 Optimization of Service Function Placement, QoS, and Multi-operator Network Sharing for Intelligent IoT Services

IoT services are mostly deployed and executed in a distributed environment. Moving a composite application to a particular environment requires a distribution of contained services before deployment. Hence, application owners want to optimize the distribution of IoT

services to improve network efficiency and user experience. A dynamic service provisioning, i.e. dynamic resource allocation, and dynamic deployment of services in a distributed environment enables high flexibility and optimized usage of the infrastructure. In particular, optimized distributions of services can be created by taking IoT network dependencies between services into account. Correlating the service dependencies and a particular state of infrastructure at deployment time leads to a best-qualified region in the infrastructure for the deployment (Gorlach and Leymann, 2012).

IoT services will have strict QoS requirements, including remote surgery via tactile internet, remote patient monitoring, drone delivery and surveillance. In these services QoS will play a vital role in determining user experience. For example, if a patient is monitored/operated on remotely or a drone is distantly maneuvered, the user experience will determine the amount of resources required to be allocated to reach user satisfaction. Hence, more adaptive and dynamic multimedia delivery methods are needed (Aazam and Harras, 2019).

Nowadays, the mobile and IoT networking world has undergone a rapid evolution. Driven by increasing demand and a highly competitive market, the choice of network providers and access technologies has significantly increased. Service offers need to provide dynamic services for mobile and IoT users at the same time. The services should support multiple services with high capacity using mobile networks, as well as low data rate, and long coverage using IoT networks (Hanafiah et al., 2012). This new demand will impact the requirements of multiple network coexistence, which becomes a challenge for researchers.

1.5.5 Data Time stamping and Clock Synchronization Services for Wide-area IoT Systems

Getting all devices in an IoT system to have a common notion of time is important to applications running on the system. This chapter discusses two basic system services achieving the common notion of time among the devices – data time stamping and clock synchronization. Data time stamping is to record the time of interest in terms of the wall clock; clock synchronization is to ensure the clocks of the devices in the system have the same value at all times (Yan et al., 2017). However, as the devices deeply embedded in the physical world face many uncertainties such as time-varying network connectivity and clock faults, ensuring accurate data time stamping and clock synchronization is challenging in practice. Atomic clocks, GPS, and clock synchronization and calibration protocols represent principal means to achieve data time stamping and clock synchronization. For massive deployments, chip-scale atomic clocks are still uneconomical solutions. Although GPS receivers can provide global time with μs accuracy, they generally do not work in indoor environments. Increased heterogeneity and limited resources in both hardware and software platforms are the key characteristics of IoT (Li et al., 2018). Since there are a large number of heterogeneous devices under the IoT access system, a number of them require different precision of clock synchronization for many situations such as data collection with space-time consistency. Therefore, how to realize the clock synchronization on IoT access system is needed urgently. On one hand, the way to access the reliable clock source according to different demands is one of the major issues. On the other hand, how to realize the clock synchronization for the heterogeneous underlying devices with different clock precision is another major issue.

1.6 Conclusion

This chapter has reviewed some well-known IoT technologies and related standards, including RFID, NFC, ZigBee, LoRa, Sigfox, and NB-IoT, as well as emerging network technologies. Their system architectures and technical advantages have been briefly discussed. Then, this chapter overviews a multiple-tier user-centered IoT network architecture, including new data collection technologies, computing power networks, and intelligent algorithms. In addition, key technologies in IoIT are introduced, such as mmWave, SDN, AI, and so on. Some applications relating to traditional IoT and IoIT are analyzed. With more and more IoT systems being deployed for different industrial sectors, it is very challenging to overcome the vertical barriers and mitigate the fragmentation problem across multiple application domains. It is also very difficult to guarantee system security and customer privacy while connecting and integrating several enterprise-level IoT platforms with heterogeneous data structures. At the end of this chapter, the requirements and challenges for intelligent IoT services are introduced.

References

Narrowband Internet of Things (NB-IoT); Technical Report for BS and UE radio transmission and reception (Release 13). https://www.3gpp.org/dynareport/36802.htm, 2017.

3GPP. Service Requirements for Machine-Type Communications (MTC). http://www.3gpp.org, 2014.

3GPP. Cellular system support for ultra-low complexity and low throughput Internet of Things (CIoT). https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2719, 2016a.

3GPP. Standardization of NB-IOT completed. https://www.3gpp.org/news-events/1785-nb_iot_complete, 2016b.

3GPP. Study on the security aspects of the next generation system. 2017.

Mohammad Aazam and Khaled A. Harras. Mapping QoE with resource estimation in IoT. In *2019 IEEE 5th World Forum on Internet of Things (WF-IoT)*. IEEE, apr 2019. doi: 10.1109/wf-iot.2019.8767254.

Nyoman Adhiarna and Jae-Jeung Rho. Standardization and global adoption of radio frequency identification (RFID): Strategic issues for developing countries. In *2009 Fourth International Conference on Computer Sciences and Convergence Information Technology*. IEEE, 2009. doi: 10.1109/iccit.2009.300.

U. Aftab and G. F. Siddiqui. Big data augmentation with data warehouse: A survey. In *2018 IEEE International Conference on Big Data (Big Data)*, pages 2785–2794, Dec 2018. doi: 10.1109/BigData.2018.8622206.

S. K. Agrawal and K. Sharma. 5g millimeter wave (mmwave) communications. In *2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom)*, pages 3630–3634, March 2016.

N. Ahmed, H. Rahman, and Md.I. Hussain. A comparison of 802.11ah and 802.15.4 for IoT. *ICT Express*, 2(3):100–102, sep 2016. doi: 10.1016/j.icte.2016.07.003.

R. R. Al-Dahhan, Q. Shi, G. M. Lee, and K. Kifayat. Revocable, decentralized multi-authority access control system. In *2018 IEEE/ACM International Conference on Utility and Cloud Computing Companion (UCC Companion)*, pages 220–225, Dec 2018. doi: 10.1109/UCC-Companion.2018.00088.

Shadi Al-Sarawi, Mohammed Anbar, Kamal Alieyan, and Mahmood Alzubaidi. Internet of things (IoT) communication protocols: Review. In *2017 8th International Conference on Information Technology (ICIT)*. IEEE, may 2017. doi: 10.1109/icitech.2017.8079928.

Zigbee Alliance. Zigbee specification. http://www.zigbee.org/wp-content/uploads/2014/11/docs-05-3474-20-0csg-zigbee-specification.pdf, 2012.

M. M. Alsulami and N. Akkari. The role of 5g wireless networks in the internet-of- things (iot). In *2018 1st International Conference on Computer Applications Information Security (ICCAIS)*, pages 1–8, April 2018. doi: 10.1109/CAIS.2018.8471687.

Olumuyiwa Oludare FAGBOHUN and. Comparative studies on 3g,4g and 5g wireless technology. *IOSR Journal of Electronics and Communication Engineering*, 9(2):133–139, 2014. doi: 10.9790/2834-0925133139.

Michael Armbrust, Armando Fox, Rean Griffith, Anthony Joseph, Randy Katz, Andy Konwinski, Gunho Lee, David Patterson, Ariel Rabkin, Ion Stoica, and Matei Zaharia. A view of cloud computing. *Commun. ACM*, 53:50–58, 04 2010. doi: 10.1145/1721654.1721672.

Alos Augustin, Jiazi Yi, Thomas Clausen, and William Townsley. A study of LoRa: Long range & low power networks for the internet of things. *Sensors*, 16(9):1466, sep 2016. doi: 10.3390/s16091466.

A. Batyuk and V. Voityshyn. Apache storm based on topology for real-time processing of streaming data from social networks. In *2016 IEEE First International Conference on Data Stream Mining Processing (DSMP)*, pages 345–349, Aug 2016. doi: 10.1109/DSMP.2016.7583573.

R. K. Behera, A. K. Sahoo, and C. Pradhan. Big data analytics in real time - technical challenges and its solutions. In *2017 International Conference on Information Technology (ICIT)*, pages 30–35, Dec 2017. doi: 10.1109/ICIT.2017.39.

Behrtech. MIOTY: The only LPWAN solution for Industrial IoT standardized by ETSI. https://behrtech.com/mioty/, 2020.

F. Benjelloun, A. A. Lahcen, and S. Belfkih. An overview of big data opportunities, applications and tools. In *2015 Intelligent Systems and Computer Vision (ISCV)*, pages 1–6, March 2015. doi: 10.1109/ISACV.2015.7105553.

Mudit Ratana Bhalla and Anand Vardhan Bhalla. Generations of mobile wireless technology: A survey. *International Journal of Computer Applications*, 5(4): 26–32, aug 2010. doi: 10.5120/905-1282.

B. Chen, J. Wan, L. Shu, P. Li, M. Mukherjee, and B. Yin. Smart factory of industry 4.0: Key technologies, application case, and challenges. *IEEE Access*,6:6505–6519, 2018a. ISSN 2169-3536. doi: 10.1109/ACCESS.2017.2783682.

C. Chen, M. Lin, and C. Liu. Edge computing gateway of the industrial internet of things using multiple collaborative microcontrollers. *IEEE Network*, 32(1): 24–32, Jan 2018b. ISSN 1558-156X. doi: 10.1109/MNET.2018.1700146.

S. Chen, J. Hu, Y. Shi, and L. Zhao. Lte-v: A td-lte-based v2x solution for future vehicular network. *IEEE Internet of Things Journal*, 3(6):997–1005, Dec 2016. ISSN 2372-2541. doi: 10.1109/JIOT.2016.2611605.

M. Chiang, S. Ha, C. I, F. Risso, and T. Zhang. Clarifying fog computing and networking: 10 questions and answers. *IEEE Communications Magazine*, 55 (4):18–20, April 2017. ISSN 1558-1896. doi: 10.1109/MCOM.2017.7901470.

H. Chien, Y. Lin, C. Lai, and C. Wang. End-to-end slicing as a service with computing and communication resource allocation for multi-tenant 5g systems. *IEEE Wireless Communications*, 26(5):104–112, October 2019. ISSN 1558-0687. doi: 10.1109/MWC.2019.1800466.

K. R. Choo, S. Gritzalis, and J. H. Park. Cryptographic solutions for industrial internet-of-things: Research challenges and opportunities. *IEEE Transactions on Industrial Informatics*, 14(8):3567–3569, Aug 2018. ISSN 1941-0050. doi: 10.1109/TII.2018.2841049.

C. Cooper, D. Franklin,M. Ros, F. Safaei, and M. Abolhasan. A comparative survey of vanet clustering techniques. *IEEE Communications Surveys Tutorials*, 19(1):657–681, Firstquarter 2017. ISSN 2373-745X. doi: 10.1109/COMST.2016.2611524.

Vedat Coskun, Busra Ozdenizci, and Kerem Ok. The survey on near field communication. *Sensors*, 15(6):13348–13405, jun 2015. doi: 10.3390/s150613348.

Laizhong Cui, Chong Xu, Shu Yang, Joshua Zhexue Huang, Jianqiang Li, Xizhao Wang, Zhong Ming, and Nan Lu. Joint optimization of energy consumption and latency in mobile edge computing for internet of things. *IEEE Internet of Things Journal*, 6(3):4791–4803, jun 2019. doi: 10.1109/jiot.2018.2869226.

P. Datta and B. Sharma. A survey on iot architectures, protocols, security and smart city based applications. In *2017 8th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, pages 1–5, July 2017. doi: 10.1109/ICCCNT.2017.8203943.

Y. Demchenko, C. de Laat, and P. Membrey. Defining architecture components of the big data ecosystem. In *2014 International Conference on Collaboration Technologies and Systems (CTS)*, pages 104–112, May 2014. doi: 10.1109/CTS.2014.6867550.

S. Dietzel, J. Petit,F. Kargl, and B. Scheuermann. In-network aggregation for vehicular ad hoc networks. *IEEE Communications Surveys Tutorials*, 16(4):1909–1932, Fourthquarter 2014. ISSN 2373-745X. doi: 10.1109/COMST.2014.2320091.

K. Dolui and S. K. Datta. Comparison of edge computing implementations: Fog computing, cloudlet and mobile edge computing. In *2017 Global Internet of Things Summit (GIoTS)*, pages 1–6, June 2017. doi: 10.1109/GIOTS.2017.8016213.

Ali Dorri, Salil S. Kanhere, Raja Jurdak, and Praveen Gauravaram. Blockchain for IoT security and privacy: The case study of a smart home. In *2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*. IEEE, mar 2017. doi: 10.1109/percomw.2017.7917634.

Shahin Farahani. *ZigBee Wireless Networks and Transceivers*. Newnes, 2011.

Laith Farhan, Sinan T. Shukur, Ali E. Alissa, Mohmad Alrweg, Umar Raza, and Rupak Kharel. A survey on the challenges and opportunities of the internet of things (IoT). In *2017 Eleventh International Conference on Sensing Technology (ICST)*. IEEE, dec 2017. doi: 10.1109/icsenst.2017.8304465.

Szymon Fedor and Martin Collier. On the problem of energy efficiency of multi-hop vs one-hop routing in wireless sensor networks. In *21st International Conference on Advanced Information Networking and Applications Workshops (AINAW'07)*, volume 2, pages 380–385. IEEE, 2007.

M. Feng, S. Mao, and T. Jiang. Base station on-off switching in 5g wireless networks: Approaches and challenges. *IEEE Wireless Communications*, 24(4): 46–54, Aug 2017. ISSN 1558-0687. doi: 10.1109/MWC.2017.1600353.

Z. Feng and Y. Zhu. A survey on trajectory data mining: Techniques and applications. *IEEE Access*, 4:2056–2067, 2016. ISSN 2169-3536. doi: 10.1109/ACCESS.2016.2553681.

Klaus Finkenzeller. *RFID Handbook: Fundamentals and Applications in Contactless Smart Cards, Radio Frequency Identification and Near-field Communication*. John Wiley & Sons, 2010.

X. Foukas, G. Patounas, A. Elmokashfi, and M. K. Marina. Network slicing in 5g: Survey and challenges. *IEEE Communications Magazine*, 55(5):94–100, May 2017. ISSN 1558-1896. doi: 10.1109/MCOM.2017.1600951.

G. Gampala and C. J. Reddy. Massive mimo – beyond 4g and a basis for 5g. *International Applied Computational Electromagnetics Society Symposium (ACES)*, pages 1–2, 2018.

Darminder Singh Ghataoura, Yang Yang, George Matich, and Selex Galileo. SWOB: Swarm intelligent odour based routing for geographic wireless sensor network applications. In *MILCOM 2009 - 2009 IEEE Military Communications Conference*. IEEE, oct 2009. doi: 10.1109/milcom.2009.5380107.

A. Ghosh, A. Maeder, M. Baker, and D. Chandramouli. 5g evolution: A view on 5g cellular technology beyond 3gpp release 15. *IEEE Access*, 7:127639–127651, 2019. ISSN 2169-3536. doi: 10.1109/ACCESS.2019.2939938.

Katharina Gorlach and Frank Leymann. Dynamic service provisioning for the cloud. In *2012 IEEE Ninth International Conference on Services Computing*. IEEE, jun 2012. doi: 10.1109/scc.2012.30.

F. Gürcan and M. Berigel. Real-time processing of big data streams: Lifecycle, tools, tasks, and challenges. In *2018 2nd International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT)*, pages 1–6, Oct 2018. doi: 10.1109/ISMSIT.2018.8567061.

H. Guo, J. Liu, J. Zhang,W. Sun, and N. Kato. Mobile-edge computation offloading for ultradense iot networks. *IEEE Internet of Things Journal*, 5(6): 4977–4988, Dec 2018. ISSN 2372-2541. doi: 10.1109/JIOT.2018.2838584.

Syazalina Mohd Ali Hanafiah, Azita Laily Yusof, Norsuzila Ya'acob, and Mohd Tarmizi Ali. Performance studies on multi-operator sharing algorithm for cellular wireless network. In *2012 International Conference on ICT Convergence (ICTC)*. IEEE, oct 2012. doi: 10.1109/ictc.2012.6387153.

Ali Hazmi, Jukka Rinne, and Mikko Valkama. Feasibility study of 802.11ah radio technology for IoT and m2m use cases. In *2012 IEEE Globecom Workshops*. IEEE, dec 2012. doi: 10.1109/glocomw.2012.6477839.

L. He, Z. Yan, and M. Atiquzzaman. Lte/lte-a network security data collection and analysis for security measurement: A survey. *IEEE Access*, 6:4220–4242, 2018. ISSN 2169-3536. doi: 10.1109/ACCESS.2018.2792534.

Jonathan Holdowsky, M Mahto, M Raynor, and M Cotteleer. A primer on the technologies building the iot, 2015.

W. Hong, K. Baek, and S. Ko. Millimeter-wave 5g antennas for smartphones: Overview and experimental demonstration. *IEEE Transactions on Antennas and Propagation*, 65(12):6250–6261, Dec 2017. ISSN 1558-2221. doi: 10.1109/TAP.2017.2740963.

Huawei. NB-IOT Enabling New Business Opportunities whitepaper. https://e.huawei.com/en/material/his/iot/6ba6590551ed4ad8b7bbe3c751fe8ea4, 2016a.

Huawei. NB-IoT White Paper. http://carrier.huawei.com/en/technical-topics/wireless-network/NB-IoT/NB-IoT-White-Paper, 2016b.

International Telecommunication Union (ITU). ITU Internet Reports 2005: The Internet of Things-Executive Summary. Nov 2005.

Iotivity. IoTivity Architecture. https://iotivity.org/about/iotivity-architecture, 2020.

V. K. Jain and S. Kumar. Big data analytic using cloud computing. In *2015 Second International Conference on Advances in Computing and Communication Engineering*, pages 667–672, May 2015. doi: 10.1109/ICACCE.2015.112.

Xiaolin Jia, Quanyuan Feng, Taihua Fan, and Quanshui Lei. RFID technology and its applications in internet of things (IoT). In *2012 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet)*. IEEE, apr 2012. doi: 10.1109/cecnet.2012.6201508.

S. Kaisler, F. Armour, J. A. Espinosa, and W. Money. Big data: Issues and challenges moving forward. In *2013 46th Hawaii International Conference on System Sciences*, pages 995–1004, Jan 2013. doi: 10.1109/HICSS.2013.645.

A. Katal, M. Wazid, and R. H. Goudar. Big data: Issues, challenges, tools and good practices. In *2013 Sixth International Conference on Contemporary Computing (IC3)*, pages 404–409, Aug 2013. doi: 10.1109/IC3.2013.6612229.

J. B. Kenney. Dedicated short-range communications (dsrc) standards in the united states. *Proceedings of the IEEE*, 99(7):1162–1182, July 2011. ISSN 1558-2256. doi: 10.1109/JPROC.2011.2132790.

L. U. Khan, I. Yaqoob, N. H. Tran,Z. Han, and C. S. Hong. Network slicing: Recent advances, taxonomy, requirements, and open research challenges. *IEEE Access*, pages 1–1, 2020. ISSN 2169-3536. doi: 10.1109/ACCESS.2020.2975072.

J. M. Khurpade, D. Rao, and P. D. Sanghavi. A survey on iot and 5g network. In *2018 International Conference on Smart City and Emerging Technology (ICSCET)*, pages 1–3, Jan 2018. doi: 10.1109/ICSCET.2018.8537340.

Mihai T Lazarescu. Design of a wsn platform for long-term environmental monitoring for iot applications. *IEEE Journal on emerging and selected topics in circuits and systems*, 3(1):45–54, 2013.

Il-Gu Lee and Myungchul Kim. Interference-aware self-optimizing wi-fi for high efficiency internet of things in dense networks. *Computer Communications*,89-90:60–74, sep 2016. doi: 10.1016/j.comcom.2016.03.008.

L. Li, S. Bagheri, H. Goote, A. Hasan, and G. Hazard. Risk adjustment of patient expenditures: A big data analytics approach. In *2013 IEEE International Conference on Big Data*, pages 12–14, Oct 2013. doi: 10.1109/BigData.2013.6691790.

Li Li, Hu Xiaoguang, Chen Ke, and He Ketai. The applications of WiFi-based wireless sensor network in internet of things and smart grid. In *2011 6th IEEE Conference on Industrial Electronics and Applications*. IEEE, jun 2011. doi: 10.1109/iciea.2011.5975693.

Yang Li, Rui Tan, and David K. Y. Yau. Natural timestamps in powerline electromagnetic radiation. *ACM Transactions on Sensor Networks*, 14(2): 1–30, jul 2018. doi: 10.1145/3199676.

Z. Liu, Z. L. Jiang, X. Wang, Y. Wu, and S. M. Yiu. Multi-authority ciphertext policy attribute-based encryption scheme on ideal lattices. In *2018 IEEE Intl Conf on Parallel*

Distributed Processing with Applications, Ubiquitous Computing Communications, Big Data Cloud Computing, Social Computing Networking, Sustainable Computing Communications (ISPA/IUCC/BDCloud/SocialCom/SustainCom), pages 1003–1008, Dec 2018. doi: 10.1109/BDCloud.2018.00146.

A. Londhe and P. P. Rao. Platforms for big data analytics: Trend towards hybrid era. In *2017 International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS)*, pages 3235–3238, Aug 2017. doi: 10.1109/ICECDS.2017.8390056.

Rongxing Lu, Kevin Heung, Arash Habibi Lashkari, and Ali A. Ghorbani. A lightweight privacy-preserving data aggregation scheme for fog computing-enhanced IoT. *IEEE Access*, 5: 3302–3312, 2017. doi: 10.1109/access.2017.2677520.

Y. Ma, Y. Chen, and J. Chen. Sdn-enabled network virtualization for industry 4.0 based on iots and cloud computing. In *2017 19th International Conference on Advanced Communication Technology (ICACT)*, pages 199–202, Feb 2017. doi: 10.23919/ICACT.2017.7890083.

P. Mach and Z. Becvar. Mobile edge computing: A survey on architecture and computation offloading. *IEEE Communications Surveys Tutorials*, 19(3):1628–1656, thirdquarter 2017. ISSN 2373-745X. doi: 10.1109/COMST.2017.2682318.

Somayya Madakam, R. Ramaswamy, and Siddharth Tripathi. Internet of things (IoT): A literature review. *Journal of Computer and Communications*, 03 (05):164–173, 2015. doi: 10.4236/jcc.2015.35021.

B. A. Martin,F. Michaud, D. Banks, A. Mosenia,R. Zolfonoon, S. Irwan, S. Schrecker, and J. K. Zao. Openfog security requirements and approaches. In *2017 IEEE Fog World Congress (FWC)*, pages 1–6, Oct 2017. doi: 10.1109/FWC.2017.8368537.

Kais Mekki, Eddy Bajic, Frederic Chaxel, and Fernand Meyer. A comparative study of LPWAN technologies for large-scale IoT deployment. *ICT Express*, 5(1):1–7, mar 2019. doi: 10.1016/j.icte.2017.12.005.

Mithun Mukherjee, Rakesh Matam, Lei Shu, Leandros Maglaras, Mohamed Amine Ferrag, Nikumani Choudhury, and Vikas Kumar. Security and privacy in fog computing: Challenges. *IEEE Access*, 5:19293–19304, 2017. doi: 10.1109/access.2017.2749422.

Geoff Mulligan. The 6lowpan architecture. In *Proceedings of the 4th workshop on Embedded networked sensors - EmNets '07*. ACM Press, 2007. doi: 10.1145/1278972.1278992.

R. Munoz, J. Mangues-Bafalluy, R. Vilalta, C. Verikoukis, J. Alonso-Zarate, N. Bartzoudis, A. Georgiadis, M. Payaro, A. Perez-Neira, R. Casellas, R. Martinez, J. Nunez-Martinez, M. Requena Esteso, D. Pubill, O. Font-Bach, P. Henarejos, J. Serra, and F. Vazquez-Gallego. The cttc 5g end-to-end experimental platform: Integrating heterogeneous wireless/optical networks, distributed cloud, and iot devices. *IEEE Vehicular Technology Magazine*, 11 (1):50–63, March 2016. ISSN 1556-6080. doi: 10.1109/MVT.2015.2508320.

C Siva Ram Murthy and BS Manoj. *Ad hoc wireless networks: Architectures and protocols, portable documents*. Pearson education, 2004.

NGMN. Description of network slicing concept. 2016.

Gianni Pasolini, Chiara Buratti, Luca Feltrin, Flavio Zabini, Cristina De Castro, Roberto Verdone, and Oreste Andrisano. Smart city pilot projects using LoRa and IEEE802.15.4 technologies. *Sensors*, 18(4):1118, apr 2018. doi: 10.3390/s18041118.

Uroš M Pešović, Jože J Mohorko, Karl Benkič, and žarko F Čučej. Single-hop vs. multi-hop–energy efficiency analysis in wireless sensor networks. In *18th Telecommunications Forum, TELFOR*, 2010.

S. Ramprasad, N. R. Shanbhag, and I. N. Hajj. Decorrelating (decor) transformations for low-power digital filters. *IEEE Transactions on Circuits and Systems II: Analog and Digital Signal Processing*, 46(6):776–788, June 1999. ISSN 1558-125X. doi: 10.1109/82.769785.

P.P. Ray. A survey on internet of things architectures. *Journal of King Saud University - Computer and Information Sciences*, 30(3):291–319, jul 2018. doi: 10.1016/j.jksuci.2016.10.003.

P. Rost, C. Mannweiler,D. S. Michalopoulos, C. Sartori,V. Sciancalepore,N. Sastry, O. Holland, S. Tayade, B. Han, D. Bega, D. Aziz, and H. Bakker. Network slicing to enable scalability and flexibility in 5g mobile networks. *IEEE Communications Magazine*, 55(5):72–79, May 2017. ISSN 1558-1896. doi: 10.1109/MCOM.2017.1600920.

David Schatsky, Craig Muraskin, and Ragu Gurumurthy. Demystifying artificial intelligence: what business leaders need to know about cognitive technologies. *A Deloitte Series on Cognitive Technologies*, 2014.

J Schlienz and D Raddino. Narrowband internet of things whitepaper. 2016.

Sigfox. Sigfox Device ARIB Mode White Paper. https://support.sigfox.com/docs/sigfox-device-arib-mode-white-paper, 2018a.

Sigfox. Sigfox Device ETSI Mode White Paper. https://support.sigfox.com/docs/sigfox-device-etsi-mode-white-paper, 2018b.

W. Sun, J. Liu, Y. Yue, and H. Zhang. Double auction-based resource allocation for mobile edge computing in industrial internet of things. *IEEE Transactions on Industrial Informatics*, 14(10):4692–4701, Oct 2018. ISSN 1941-0050. doi: 10.1109/TII.2018.2855746.

C. K. Toh. *Wireless ATM and ad-hoc networks*. Kluwer Academic Press, 1997.

Chai K Toh. *Ad hoc mobile wireless networks: protocols and systems*. Pearson Education, 2001.

Riccardo Trivisonno, Xueli An, and Qing Wei. Network slicing for 5g systems: A review from an architecture and standardization perspective. pages 36–41, 09 2017. doi: 10.1109/CSCN.2017.8088595.

International Telecommunication Union. Overview of the Internet of things. http://handle.itu.int/11.1002/1000/11559, 2016.

R. van Kranenburg and S. Dodson. *The Internet of Things: A Critique of Ambient Technology and the All-seeing Network of RFID*. Network notebooks. Institute of Network Cultures, 2008. ISBN 9789078146063. URL https://books.google.com/books?id=PilgkgEACAAJ.

C Vedat, Kerem Ok, and O Busra. Near field communication: From theory to practice. *Istanbuh NFC Lab-lstanbul, ISIK University*, pages 82–94, 2012.

R. Vilalta,A. Mayoral,D. Pubill, R. Casellas, R. Martínez, J. Serra, C. Verikoukis, and R. Muñoz. End-to-end sdn orchestration of iot services using an sdn/nfv-enabled edge node. In *2016 Optical Fiber Communications Conference and Exhibition (OFC)*, pages 1–3, March 2016.

J. Wang,J. Liu, and N. Kato. Networking and communications in autonomous driving: A survey. *IEEE Communications Surveys Tutorials*, 21(2):1243–1274, Secondquarter 2019a. ISSN 2373-745X. doi: 10.1109/COMST.2018.2888904.

P. Wang, C. Yao,Z. Zheng, G. Sun, and L. Song. Joint task assignment, transmission, and computing resource allocation in multilayer mobile edge computing systems. *IEEE Internet of Things Journal*, 6(2):2872–2884, April 2019b. ISSN 2372-2541. doi: 10.1109/JIOT.2018.2876198.

P. Wang, Z. Zheng, B. Di, and L. Song. Hetmec: Latency-optimal task assignment and resource allocation for heterogeneous multi-layer mobile edge computing. *IEEE Transactions on Wireless Communications*, 18(10):4942–4956, Oct 2019c. ISSN 1558-2248. doi: 10.1109/TWC.2019.2931315.

B. Yadranjiaghdam, N. Pool, and N. Tabrizi. A survey on real-time big data analytics: Applications and tools. In *2016 International Conference on Computational Science and Computational Intelligence (CSCI)*, pages 404–409, Dec 2016. doi: 10.1109/CSCI.2016.0083.

Zhenyu Yan, Yang Li, Rui Tan, and Jun Huang. Application-layer clock synchronization for wearables using skin electric potentials induced by powerline radiation. In *Proceedings of the 15th ACM Conference on Embedded Network Sensor Systems*. ACM, nov 2017. doi: 10.1145/3131672.3131681.

Yang Yang. Multi-tier computing networks for intelligent iot. *Nature Electronics*, 2, 01 2019. doi: 10.1038/s41928-018-0195-9.

Yang Yang, Hui hai Wu, and Hsiao hwa Chen. SHORT: Shortest hop routing tree for wireless sensor networks. In *2006 IEEE International Conference on Communications*. IEEE, 2006a. doi: 10.1109/icc.2006.255606.

Yang Yang, Feiyi Huang, Xuanye Gu, Mohsen Guizani, and Hsiao-Hwa Chen. Double sense multiple access for wireless ad hoc networks. In *Proceedings of the 3rd international conference on Quality of service in heterogeneous wired/wireless networks - QShine 06*. ACM Press, 2006b. doi: 10.1145/1185373.1185386.

Yang Yang, Jing Xu, Guang Shi, and Cheng-Xiang Wang. *5G Wireless Systems*. Springer International Publishing, 2018. doi: 10.1007/978-3-319-61869-2.

C. Yao,X. Wang,Z. Zheng, G. Sun, and L. Song. Edgeflow: Open-source multi-layer data flow processing in edge computing for 5g and beyond. *IEEE Network*, 33(2):166–173, March 2019. ISSN 1558-156X. doi: 10.1109/MNET.2018.1800001.

J. Yin and D. Zhao. Data confidentiality challenges in big data applications. In *2015 IEEE International Conference on Big Data (Big Data)*, pages 2886–2888, Oct 2015. doi: 10.1109/BigData.2015.7364111.

S. Yu, M. Liu, W. Dou, X. Liu, and S. Zhou. Networking for big data: A survey. *IEEE Communications Surveys Tutorials*, 19(1):531–549, Firstquarter 2017. ISSN 2373-745X. doi: 10.1109/COMST.2016.2610963.

Y. Yu. Mobile edge computing towards 5g: Vision, recent progress, and open challenges. *China Communications*, 13(Supplement2):89–99, N 2016. ISSN 1673-5447. doi: 10.1109/CC.2016.7833463.

Morteza M Zanjireh and Hadi Larijani. A survey on centralised and distributed clustering routing algorithms for wsns. In *2015 IEEE 81st Vehicular Technology Conference (VTC Spring)*, pages 1–6. IEEE, 2015.

Morteza M Zanjireh, Ali Shahrabi, and Hadi Larijani. Anch: A new clustering algorithm for wireless sensor networks. In *2013 27th International Conference on Advanced Information Networking and Applications Workshops*, pages 450–455. IEEE, 2013.

S. Zhang. An overview of network slicing for 5g. *IEEE Wireless Communications*, 26(3):111–117, June 2019. ISSN 1558-0687. doi: 10.1109/MWC.2019.1800234.

Y. Zhang, B. Di,P. Wang, J. Lin, and L. Song. Hetmec: Heterogeneous multi-layer mobile edge computing in the 6g era. *IEEE Transactions on Vehicular Technology*, pages 1–1, 2020. ISSN 1939-9359. doi: 10.1109/TVT.2020.2975559.

Cheng Zhao, Wuxiong Zhang, Yang Yang, and Sha Yao. Treelet-based clustered compressive data aggregation for wireless sensor networks. *IEEE Transactions on Vehicular Technology*, 64(9):4257–4267, sep 2015. doi: 10.1109/tvt.2014.2361250.

C. Zhong, Z. Zhu, and R. Huang. Study on the iot architecture and gateway technology. In *2015 14th International Symposium on Distributed Computing and Applications for Business Engineering and Science (DCABES)*, pages 196–199, Aug 2015. doi: 10.1109/DCABES.2015.56.