







Review

Internet of Things: A Comprehensive Overview on Protocols, Architectures, Technologies, Simulation Tools, and Future Directions

Mohammad Mansour¹, Amal Gamal¹, Ahmed I. Ahmed¹, Lobna A. Said¹, Abdelmoniem Elbaz², Norbert Herencsar^{3,*} and Ahmed Soltan¹

¹ Nanoelectronics Integrated Systems Center (NISC), Nile University, Giza 12588, Egypt; mmansour@nu.edu.eg (M.M.); a.gamal2165@nu.edu.eg (A.G.); ah.ahmed@nu.edu.eg (A.I.A.); lsaid@nu.edu.eg (L.A.S.); asoltan@nu.edu.eg (A.S.)

² El Sewedy Electrometer Group, Cairo 12451, Egypt; amohamed@sewedy.com.eg

³ Department of Telecommunications, Faculty of Electrical Engineering and Communication, Brno University of Technology, Technicka 12, 616 00 Brno, Czech Republic

* Correspondence: herencsn@ieee.org

Abstract: The Internet of Things (IoT) is a global network of interconnected computing, sensing, and networking devices that can exchange data and information via various network protocols. It can connect numerous smart devices thanks to recent advances in wired, wireless, and hybrid technologies. Lightweight IoT protocols can compensate for IoT devices with restricted hardware characteristics in terms of storage, Central Processing Unit (CPU), energy, etc. Hence, it is critical to identify the optimal communication protocol for system architects. This necessitates an evaluation of next-generation networks with improved characteristics for connectivity. This paper highlights significant wireless and wired IoT technologies and their applications, offering a new categorization for conventional IoT network protocols. It provides an in-depth analysis of IoT communication protocols with detailed technical information about their stacks, limitations, and applications. The study further compares industrial IoT-compliant devices and software simulation tools. Finally, the study provides a summary of the current challenges, along with a broad overview of the future directions to tackle the challenges, in the next IoT generation. This study aims to provide a comprehensive primer on IoT concepts, protocols, and future insights that academics and professionals can use in various contexts.

Keywords: Internet of Things; communication protocols; application layer protocols; network simulation tools; IoT comparison; IoT hardware; IoT challenges; hybrid IoT protocols



Citation: Mansour, M.; Gamal, A.; Ahmed, A.I.; Said, L.A.; Elbaz, A.; Herencsar, N.; Soltan, A. Internet of Things: A Comprehensive Overview on Protocols, Architectures, Technologies, Simulation Tools, and Future Directions. *Energies* **2023**, *16*, 3465. <https://doi.org/10.3390/en16083465>

Academic Editors: Chun-Yen Chang, Teen-Hang Meen, Charles Tijus and Po-Lei Lee

Received: 3 March 2023

Revised: 31 March 2023

Accepted: 12 April 2023

Published: 14 April 2023



Copyright: © 2023 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

The Internet of Things has become vital to sustained economic development [1]. It turns buildings, such as homes, workplaces, factories, and even whole cities, into autonomous, self-regulating systems that do not need human help. They communicate with the physical world via actuation, sensing, and management, using current internet protocols to facilitate data transmission, analytics, and decision-making [2]. At present, it is almost impossible to think of a domain of life where IoT technology is not applicable [3]. IoT is powered by the growth of smart systems, which are enabled by a broad range of wireless technologies, such as wireless fidelity (Wi-Fi), Zigbee, and Bluetooth, as well as integrated actuators and sensors. This results in the development of enormous volumes of data, which must be processed, stored, and displayed in a way that is effective, simple, and seamless [4]. The Internet of Things has matured beyond its infancy and is transitioning from the present conventional internet to the fully comprehensive internet of the upcoming decades. The IoT revolution has increased connections among things, at a size and speed that have never

before been possible, to produce an intelligent environment [5]. Such applications' various requirements and limitations (extensibility, accessibility, and power) lead to an overall heterogeneity. Furthermore, many studies, industries, and businesses are working on different IoT features to meet the growing technological needs of such rapid growth. Therefore, several protocols have been developed to accommodate various purposes, whereby each vendor endeavors to dominate the market for the suggested devices and protocols. Manufacturers are always under market demand to provide their services in the shortest time. Therefore, rapid development is necessary to launch items early, pushing security into the future. Furthermore, these items are applied in the modern environment, living spaces, and essential infrastructural facilities (healthcare, transportation, and industrial) [6]. One of the primary areas of investigation is the need for reduced power utilization among the devices used in IoT-based systems. In addition, examining potential communication protocols has revealed promising opportunities for improvement [3].

1.1. Motivations

Multiple protocols have recently emerged due to the expansion of IoT applications and operations. Each protocol aims to either satisfy the needs of a single use case or communicate effectively throughout the whole IoT ecosystem. This evolving series of protocols produces several sets of rules and guidelines. Unfortunately, many of these documents are complicated; some may even be private and inaccessible to the general public. Therefore, it is difficult to pick the optimal communication protocol for a new design, and a poor choice might result in late production and increased design expenditure [7]. Additionally, the fundamental protocols of IoT are constantly developing, either due to the introduction of new protocols or the updating of existing versions. This results in heterogeneous deployments, where either various protocols are utilized on IoT layers or future protocols are used in conjunction with obsolete protocols. On the other hand, a limited number of studies provide a convenient simulation tool to evaluate recent versions and the required hardware for evaluation and implementation.

1.2. Related Work

Numerous articles offer comparative methodologies and analyze multiple aspects of the IoT, including its different architectures and techniques. According to a recent meta-review, the IoT and its subtopics are of intense interest to scientists working in both academic and industrial institutes [8]. Identified trends divide recent publications in this field into the following eight novel categories: IoT applications, security technologies, data, communication, communication networking, protocol standards, and development. In this section, surveys and their coverage, related to our work, are discussed.

Concerning architectures and techniques, an overview of the IoT model is provided in [9], which outlines its essential concepts and highlights critical developments in relevant studies and technological contexts. Furthermore, several security issues were investigated, followed by a brief discussion of potential IoT applications and their effects on various areas. A few applications that could be realized using IoT technology were investigated in [10]. Several IoT platform designs were examined, and a generic IoT standard paradigm was developed in [11]. Another overview of technologies was provided in [12], which studied potential conceptual models, communication technologies, difficulties, and unanswered questions. Additionally, a new six-layer design was introduced to protect the IoT infrastructure. Throughout the analysis of each protocol's specifications, a comprehensive survey of the application layer protocols, in terms of their characteristics, was presented in [7]. The results analyzed how well each protocol served the specified categories of various applications and their respective communication needs. A review of the essentials of the IoT ecosystem and communication protocols, developed primarily for IoT technology, was provided in [13]. An overview of current IoT models, techniques, and critical open-source platforms and applications was provided in [14].

Regarding the IoT protocols, the unique qualities of wireless technologies and issues with their IoT integration were presented in [15]. The study focused on Bluetooth low energy, ZigBee, Long Range (LoRa), and several other Wi-Fi variants. The problem of selecting the best technology for a particular application was investigated in [16], which compared the standard IoT communication protocols utilizing various parameters. The following are some of the criteria to be considered in selecting the best technology: topology, cryptography, power consumption, standards, frequency ranges, data rate, features, security, and coverage. The constraints and deficiencies of present security techniques were studied in [17]. Link, transport, networking, and session layers for IoT communications protocols were the main focus in [18]. Insights into the various administrative and security mechanisms for machine-to-machine (M2M) and IoT devices are provided. The study focused on specific aspects of Internet of Things networks, including communication and security protocols. An extensive summary was provided in [19] of recent developments in the application layer of the IoT and the lightweight protocols required for them to function. Nevertheless, the scope of the survey was limited to communication protocols in the IoT application layer. A description of a number of standardized protocols at a variety of networking abstraction levels, especially those designed for embedded devices with constrained resources, was offered in [20]. However, the protocols are developing and the most recent versions need to be reviewed.

1.3. Research Gaps and Contributions

Motivated by the points mentioned in Section 1.1, this work was conducted so as to cover the research gaps and to develop a unified framework wherein to compare different IoT protocols and outdated discussions on the current challenges and future directions of the IoT. This paper investigated the IoT paradigm's significant components, including its architecture, protocols, tools, and applications. A presentation is provided for wireless protocols, including the following: Zigbee, Bluetooth Low Energy (BLE), Z-wave, Wi-Fi, IPv6 over Low-power Wireless Personal Area Networks (6LoWPAN), Wi-SUN, LoRa, Long Range Wide Area Networks (LoRaWAN), NarrowBand-Internet of Things (NB-IoT). Wired protocols, such as Power Line Communication (PLC), in addition to hybrid technology, are also presented. Furthermore, a general method for comparing the IoT protocols' stack, based on the basic Open Systems Interconnection (OSI) stack, is offered. Moreover, we provide additional guidance on protocol choice and application to round out the comparison. We then compare the professional IoT hardware modules and simulation tools for various IoT protocols. Finally, a detailed discussion is provided on future directions in reshaping the IoT paradigm in the Sixth Generation (6G) era to address the present challenges. Overall, this work aims to provide a valuable overview for researchers and professionals interested in learning more about IoT methods and protocols to use in several applications.

1.4. Outline

The study is organized as shown in Figure 1. An overview of IoT, including its definition and functional building elements, is presented in Section 2. An investigation of the IoT system architecture and stack is introduced in Section 3. The different application layer protocols are investigated in Section 4. The infrastructural protocols, including wireless, wired, and hybrid communication technologies, are provided in Section 5. Industrial IoT-compliant devices for the different protocols are compared in Section 6. Simulation tools used in IoT and Wireless Sensor Networks (WSNs) are discussed in Section 7. The current challenges and open issues facing the IoT are summarized in Section 8. The state-of-the-art technologies that can be integrated into the IoT paradigm to tackle the challenges in the 6G era are introduced in Section 9. A discussion of the study's findings, including forward-looking insights, is provided in Section 10. Finally, in Section 11, the conclusions of this work are presented.

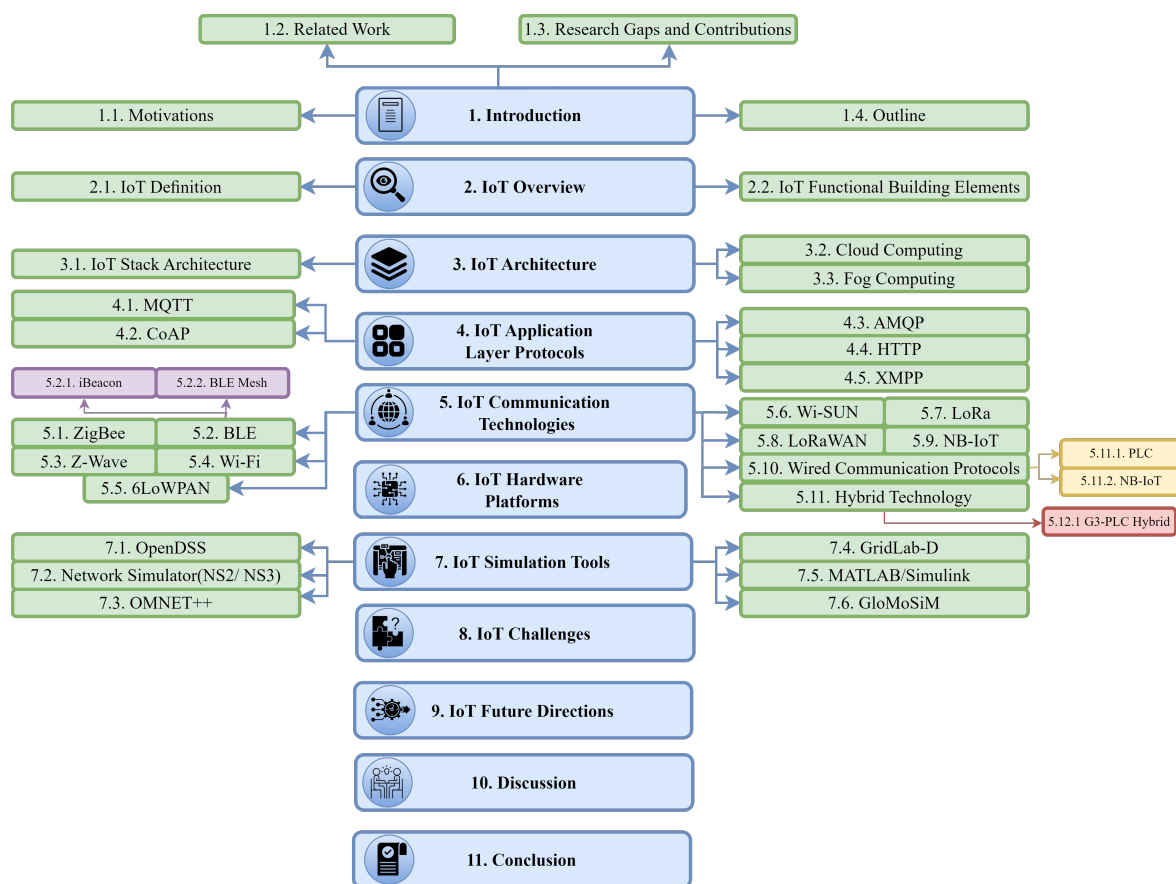


Figure 1. Article structure.

2. IoT Overview

The Internet of Things has facilitated discoveries, inventions, and interactions between things and people. These advancements enhance human quality of life and the exploitation of finite resources. Various IoT definitions and functional building blocks are discussed in this section.

2.1. IoT Definition

The business and academic worlds have recently become very interested in IoT, primarily due to the capabilities that IoT provides. It creates a world where all smart devices and technologies are linked to the Internet and capable of communicating with one another with the least amount of human interference [21]. Unfortunately, there is no agreed-upon definition for the term “IoT”, since definitions are introduced from many interpretations and viewpoints. The following definitions come from several researchers:

- Definition I: Things that are interconnected and actively involved in what can be referred to as the future internet [22].
- Definition II: There are two terms in this expression: Things refers to all devices interconnected to a network relying on identical protocols, whereas the Internet is described as the global network of many networks [5].
- Definition III: The IoT concept is any device that is always available to be accessed by anyone, at any moment, from any location, via any application, and over any network [23].

2.2. The IoT Functional Building Elements

There are several fundamental building blocks in the IoT that make it easier for smart devices to perform tasks, including sensing, actuation, identification, organization, and networking.

Sensing Devices: The core components of the IoT system are smart devices capable of carrying out a wide range of tasks, including sensing, monitoring, controlling, and actuation activities. Any IoT unit requires a variety of interfaces to connect to other smart devices, such as the following: interfaces for Internet access, Audio/Video (A/V), sensing Input/Output (I/O), and memory and storage ports are among these. In addition, IoT devices vary depending on the purpose for which each device is used, including the following examples: Smartwatches, wearable sensors, vehicles, industrial equipment, Light Emitting Diode (LED) lights, etc. [23].

Management: Remote management, either with or without human intervention, is the primary characteristic of an IoT device that sets it apart from conventional devices that are handled and controlled through mechanical switches or buttons. Additionally, IoT devices can send and receive data so that a suitable decision can be made [24].

Services: IoT applications range from workplace automation and household appliances to production lines and product tracking, among many other uses. These services can be identity-related, information-aggregating, device modeling, device discovery, device control, collaborative awareness, ubiquitous, data analytics, and data publishing services.

Security: Network data, particularly that of wireless networks, is vulnerable to a wide range of attacks, including denial of service, spoofing, eavesdropping, and so on [25]. In an attempt to counteract these assaults, IoT systems include security features, such as content integrity, message integrity, privacy, authorization, and authentication [26].

Application: The application layer offers interfaces to IoT users so they may monitor and manage various IoT applications. Furthermore, they allow users to assess and view the status of IoT systems at any time and from any location to take appropriate actions.

3. The IoT Architecture

The IoT paradigm was initially developed in largely heterogeneous situations where information could be collected from several resources and handled by various technologies in a heterogeneous environment [27]. Therefore, similar approaches, functionalities, and services can be grouped into the same layer in each proposed IoT model. This makes it easier to develop and improve the architecture of each layer in the future. Although the three-layer design adequately captures the overall concept of the IoT, it is insufficient for research on the IoT, which often concentrates on the deeper points of the Internet of Things [28].

3.1. IoT Stack Architecture

The IoT stack is divided into five layers: physical, data link, network, transport, and application layers. These layers are depicted in Figure 2.

The physical layer is also known as the “perception layer” or “recognition layer” in the context of the IoT. The primary function of the physical layer is to sense the physical characteristics of the surrounding objects. It relies on various sensing technologies, such as Radio Frequency Identification (RFID), WSN, and the Global Positioning System (GPS) [12]. Additionally, it is in charge of turning the information into digital signals, which are easier to transmit via a network. Nanotechnologies and embedded intelligence are crucial to the physical layer [29]. The first produces smaller chips inserted into everyday objects, such as nano-integrated wearable devices [30]. The second one provides them with the computing power that any upcoming applications need. The Data Link Layer’s primary features are packet boundary distinction, frame synchronization, sender and destination address management, error detection in the physical media channel, and collision prevention [31]. In addition, each protocol has unique features ensuing from its design and implementation, including media access control mechanisms, transfer speeds, communication topology

among units, coverage distance, power utilization, and many more. The network layer provides data routing channels so that data can be sent as packets throughout the network [32]. It includes all network equipment, such as switches and routers, necessary for proper Third Generation (3G), Fourth Generation (4G), Fifth Generation (5G), Wi-Fi, infrared technology, ZigBee, and communication and routing protocols. The transport layer collaborates with the application layer to transmit and receive data without errors. It offers capabilities including packet delivery order, congestion avoidance, multiplexing, byte orientation, data integrity, and reliability for the sent data [33]. The application layer serves as the IoT architecture's front end, where most of the technology's potential is realized. It provides IoT developers with access to the platforms, interfaces, and tools they need to build IoT applications, such as those for smart homes, intelligent transportation, smart health, etc.

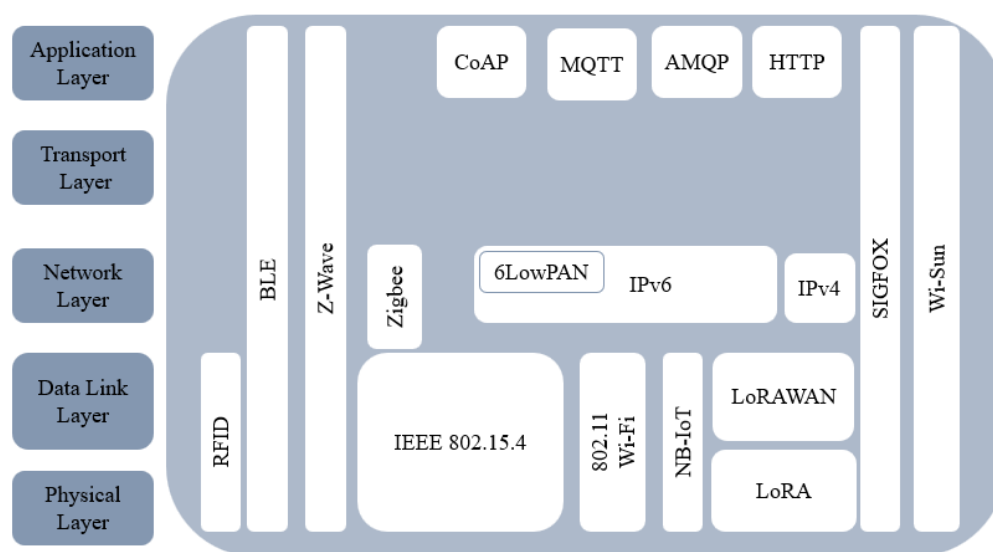


Figure 2. IoT Stack Architecture.

3.2. Cloud Computing

The IoT paradigm integrates data and connectivity infrastructure into our surroundings. This results in the creation of enormous amounts of data, which must be displayed, interpreted, and maintained in a format that is effective, convenient, and simple to recognize. In the cloud model, data processing is delegated to a network of remote servers in the cloud [34]. In this centric design, the cloud is considered the heart, with applications built on top and a network of smart devices below. Cloud computing is preferred for its ability to provide flexibility and scalability, offering infrastructure, platforms, software, and storage services. Moreover, the cloud allows programmers to exchange resources for high-performance applications, deep learning models, and analytical tools. It offers a high-performance platform in dynamic resource allocation, universal accessibility, and composability, all of which are critical for the success of upcoming IoT extensions. This platform performs a variety of functions, including receiving information from smart objects, acting as a computer that analyzes and interprets various sorts of data, and providing web-based visualizations.

Several studies have attempted to build a descriptive architecture to define the cloud computing model [35]. Three levels make up this paradigm, with the first being the base layer, which has a database that contains information on every smart device. Following this comes the component layer, which contains the software necessary to communicate with all IoT elements, to utilize some of them to carry out a task or to monitor their condition. Finally, there is the application layer, which is responsible for delivering the desired services to end users.

IoT architecture built on the cloud computing model primarily consists of the physical layer, gateway layer, and cloud services. The physical layer is used to collect data from networked devices [36]. The gateway layer contains network data, such as Local Area Network (LAN), Wide Area Network (WAN), etc. It transforms data and prepares the supplied raw data for cloud services. Cloud services are the central and crucial component of cloud-based architecture [37], responsible for applying data analytical algorithms to execute the data. The essential elements of cloud services are broker and message queues, databases, servers, and event administrators.

The key benefits of the cloud computing paradigm are still the “enormous” storage and processing capabilities, lower capital costs, and smaller ecological footprint. Nevertheless, there are significant challenges associated with this technology, including security concerns, delayed service, and limited bandwidth, in addition to increased latency and jitter when portable devices load the resources computing services [38].

3.3. Edge and Fog Computing

“Edge computing” and “fog computing” are frequently considered synonyms. However, “edge computing” is a more general term and precedes “fog computing” [36]. Recently, there has been a trend toward adopting edge computing as an alternative type of system architecture [39]. Edge computing can be defined as a computing approach that makes use of resources at the periphery of a network, while fog computing is a hybrid computing approach that makes use of both on-site resources and cloud services [40], wherein sensors and gateways play a role in data computation and analysis [41]. The major advantage of a distributed fog model over a centralized cloud architecture is its ability to support real-time and latency-sensitive IoT systems that make instant decisions, including autonomous cars, augmented and virtual reality (VR) equipment, and security tools. Owing to the delays encountered, these systems cannot accept transference of their data to be handled on a cloud platform. Edge computing brings the computation closer to the nodes at the network’s edge to provide a minimal delay [42]. Fog architecture involves several layers, including monitoring, pre-processing, storing, and security, that are placed between the physical and transport layers [43]. The monitoring layer tracks power, availability, performance, and status. The pre-processing layer filters, processes, and analyzes cloud-let data. Data backup, redistribution, and caching are all services provided by the short-term storage layer. Lastly, the security layer handles decryption and encryption, protecting sensitive information and preventing unauthorized access. Both monitoring and pre-processing occur at the cloud-let before the data is transmitted to the cloud. Edge resources differ from cloud resources in that they include inherent heterogeneity, a non-deterministic load, continuously scaling data, unpredictable links, and multi-tenancy among end users. These challenges need unique approaches to management [44]. Managing the process becomes even more difficult when real-time scenarios compete for busy resources amid unbalanced workloads. Resource management includes activities such as allocating and scheduling resources, offloading tasks, deploying services where they are most needed, and balancing workloads [45].

With edge computing, machine learning (ML) can be deployed closer to the edge of the network, where the raw data is being produced. Improvements in fog computing productivity and efficiency can be achieved by employing edge intelligence and analytical tools [46]. Edge computing that is driven by artificial intelligence may cause significant shifts in several industries. By 2025, the International Data Corporation (IDC) estimates there will be 150 billion smart edge devices available worldwide [47]. Although some kinds of edge computing are currently in use, analysts predict that this volume will increase [48]. There has been remarkable advancement in the use of artificial intelligence (AI), instead of heuristic and meta-heuristic methods, to enhance task scheduling [49]. A more detailed discussion of AI and edge computing integration is provided in Section 9.

4. IoT Application Layer Protocols

4.1. Message Queue Telemetry Transport (MQTT)

The MQTT protocol enables messages to be transmitted and received without the sender or recipient being aware of who is sending or receiving the data. Three primary components make up the MQTT: a publisher, a subscriber, and a broker [50]. In MQTT, the publisher (server) and subscriber (clients) do not need to be aware of the identities of one another. Since MQTT supports server-side processing, it is suitable for IoT devices with constrained processing and storage capabilities. Due to its ability in controlling large and small devices, MQTT is flexible and straightforward to utilize [51]. Two agents are present in every MQTT connection: clients and the broker, which acts as a server. Devices used for communication are known as “clients”. The subscriber (client) requests a message from the publisher (server) to get information. Then, a client can connect to the specified server with the broker’s help. The client in this scenario might be anything, including a sensor, a mobile device, etc. The broker controls the flow of information and is primarily responsible for collecting all publisher messages, sorting them, choosing the subscribers, and sending the messages to all customers who have subscribed. Healthcare applications frequently utilize MQTT.

4.2. Constrained Application Protocol (CoAP)

The Internet Engineering Task Force (IETF) Constrained RESTful Environments Working Group created the CoAP as a web transfer protocol for constrained devices with limited capabilities [52]. The CoAP takes advantage of a portion of Hypertext Transfer Protocol (HTTP) features. The resource limitations of many IoT devices have led to reconsidering certain HTTP functionalities. The IoT application-specific protocols can be developed by modifying HTTP’s underlying technologies. Many IoT devices, including cellphones and RFID sensors, act as CoAP clients. The CoAP server receives the data produced by these clients ubiquitously. The CoAP server transmits this data to the REST CoAP Proxy. A firewall connection is created to enable communication between the CoAP environment and the rest of the Internet. The CoAP is commonly used in smart home applications.

4.3. Advanced Message Queuing Protocol (AMQP)

The AMQP is a global standard International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 19464, created by OASIS, that offers queuing, message orientation, point-to-point routing, publish/subscribe, security, and dependability. A stable and effective message queue is the foundation of the publish/subscribe mechanism known as AMQP [53]. By utilizing the name of this exchange, publishers and customers may locate one another. The consumer then creates a “queue” and connects it to the exchange.

4.4. HTTP

The text-based and web-based HTTP is a communication protocol that provides request/response RESTful features where the client communicates with the server by sending an HTTP request message [54]. Since HTTP depends on Transmission Control Protocol (TCP) as a transport protocol and TCP as a transport protocol and Transport Layer Security/Secure Sockets Layer (TLS/SSL) as a security protocol, communication between the server and the client is connection-based. On the other hand, an IoT connection using the HTTP protocol consumes many network resources and incurs overheads because it requires the sending of several tiny packets.

4.5. Extensible Messaging and Presence Protocol (XMPP)

The XMPP is a communication protocol built on eXtensible Markup Language (XML). Developed to expand HTML, XMPP enables the insertion of unique tags and online features. It offers extensionality and data organization mechanisms as a part of HTML. For real-time communication, such as instant messaging, presence, multi-party chats, phone and video

calls, collaboration, content syndication, etc., XMPP has traditionally been utilized. The IoT real-time and scalable networking between devices or objects is made possible by the utilization of XMPP [55]. The objects (devices) have one or more nodes, and each node has several fields (of information). Each field has a value that may be read and written. The nodes must send and accept friendship requests from one another. One node can start receiving updates from another node after the other node accepts the friendship request from the first node. If a second node wants to receive updates from the first node, it must issue a friendship request and acquire approval. A dual subscription is used when both nodes become friends with one another over the network; otherwise, a single-sided subscription is used. One node can read or write field values in the other node, and data is exchanged between them on a one-to-one basis [56].

5. IoT Communication Technologies

In some IoT applications, the available technological options are constrained by the hardware capabilities, the need for low-power consumption, and the total cost of the device. Achieving low power consumption is a crucial prerequisite for developing the IoT. In addition to reduced power consumption, there are additional needs that must be taken into account. Cost of technology, security, ease of use and management, and wireless data rates and ranges, among other factors, are just a few examples of crucial needs that need to be taken into consideration. Many developing wireless technologies, like ZigBee and Bluetooth, compete to offer the IoT a low-power wireless communication option. The Institute of Electrical and Electronics Engineers (IEEE) IEEE 802.11ah, LoRa, and 6LoWPAN protocols, among others, are emerging as other wireless technologies. Figure 3 compares the distance coverage, rates, ranges, and power consumption of various wireless communication systems. In this section, IoT Protocol stacks are introduced and compared, based on their performance criteria. The reduced OSI stack is used for categorization, wherein the presentation and session layers are omitted as they have no role in IoT akin to the ones in Information Technology (IT) networks.

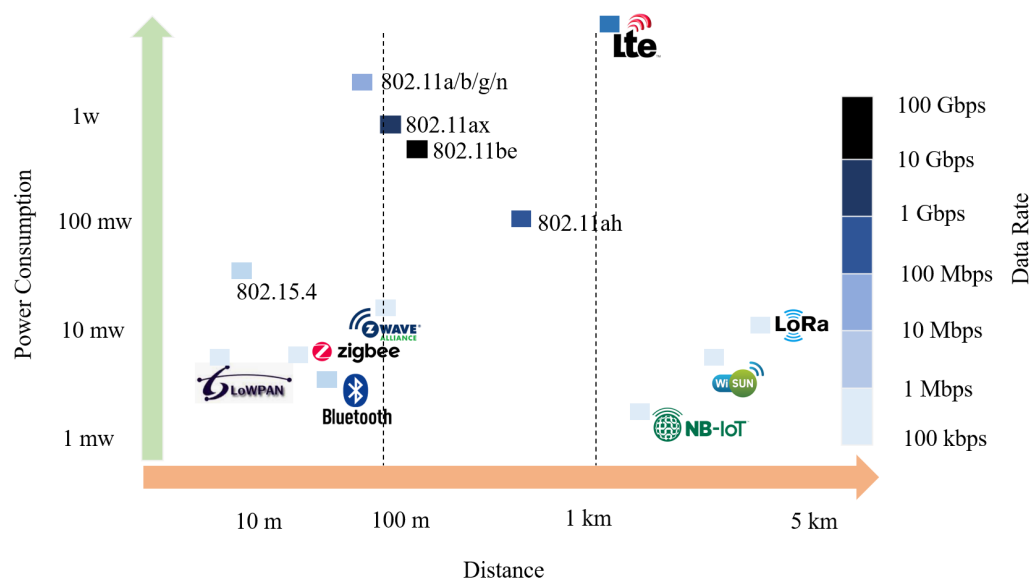


Figure 3. Power consumption, coverage distance, and data rate for the different protocols.

5.1. ZigBee

ZigBee was created when the IEEE 802.15.4 standard was approved in 2004, to be utilized in Personal Area Networks (PAN). Therefore, ZigBee is more suitable for sensors and control devices. It uses 868 MHz in Europe, 915 MHz in the United States, and 2.4 GHz everywhere else. The protocol stack’s physical layer (PHY) and Media Access layer (MAC) are defined by the IEEE 802.15.4 standard. In contrast, the ZigBee Alliance determines the

network and application layers, as shown in Figure 4. It provides a data rate of 20 kbps at 868 MHz, 40 kbps at 915 MHz, and 250 kbps at 2.4 GHz [57]. ZigBee uses Direct Sequence Spread Spectrum (DSSS) as one of its key modulation techniques to transmit data wirelessly. DSSS works by spreading the signal across a wide range of frequencies, using a unique code to encode each bit of the data. It ranges to 100m and provides low power consumption. The Zigbee PRO Standard expands the capabilities of Zigbee networks to include child device management, enhanced security, and alternative network topologies [58]. The process of adding new devices to connectivity has been made, additionally, more streamlined and consistent thanks to Base Device Behavior (BDB). Moreover, Zigbee 3.0 bundles all profile clusters into a single standard, Zigbee Cluster Library (ZCL) v7. To prevent collisions in the shared communication medium, ZigBee employs Carrier Sense Multiple Access with the Collision Avoidance (CSMA/CA) technique. This ensures that the signal detects an idle channel before transmitting data, reducing the probability of collisions and enhancing the overall reliability of the network [59]. ZigBee requires the usage of a block cipher that uses the Advanced Encryption Standard (AES) and a 128-bit key. ZigBee has many applications, such as home automation, industrial control systems, and medical data collection [60].

Figure 5 shows the three primary Zigbee system structure devices: coordinator, router, and end device. The coordinator is responsible for information management during data transmission and reception. The router serves as an intermediary device, allowing data to pass through. The end device and the parent node have only a few features to use to communicate using battery power. A ZigBee network can have a star, tree, or mesh network topology [61]. The features of ZigBee are low power consumption, low cost, fast response, less interference, self-organization, multiple topologies, and high security. The main advantage of ZigBee is the low data rate and small memory size.

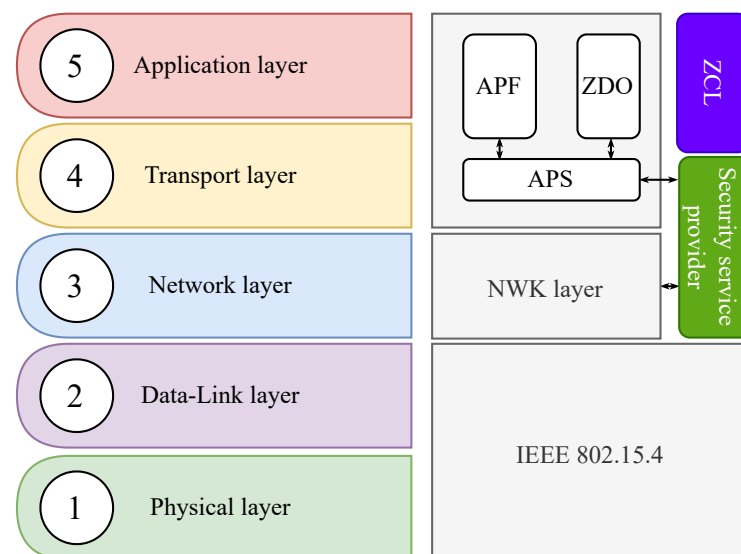


Figure 4. Comparing ZigBee stack with OSI stack.

5.2. BLE

In 1994, Bluetooth was originally invented by Ericsson, and the first description was published in 2001. The IEEE gave it the 802.15.1 standard in 2002 [62]. Bluetooth has evolved through multiple generations from 2.0, passing from the introduction of the low energy (LE) in Bluetooth version 4.0 to the current Bluetooth version 5.3 [63]. The BLE version 4.0 has a coverage distance of up to 100 m, whereas it can reach up to 400 m in version 5.0 [64]. Furthermore, BLE provides encryption and authentication techniques based on 128-bit Advanced Encryption Standard-Counter with CBC-MAC (AES-CCM) and Connection Signature Resolving Key (CSRK), respectively. It enforces two main security modes, along with a mixed security mode [65].

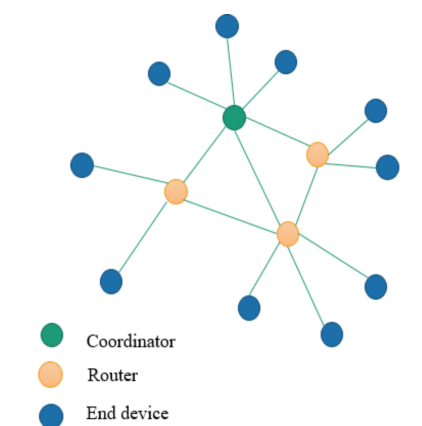


Figure 5. Zigbee Network.

The first generation of Bluetooth Basic Rate/Enhanced Data Rate (BR/EDR) was exclusively intended for sharing files via an asynchronous connectionless method. Its connection is a single point-to-multiple point connection that can accommodate both symmetrical and asymmetrical connections and is used for data broadcasting [66]. Figure 6 shows the protocol stack of Bluetooth BR or EDR. There are 79 channels, each with a 1 MHz bandwidth, making up the Bluetooth Industrial, Scientific, and Medical (ISM) band at 2.4 GHz. Bluetooth Class protocol's Radio frequency (RF) layer Frequency Shift Keying (FSK) is a modulation method representing a digital 0 and 1 by changing through two unique frequencies inside the assigned band. BR uses a variation of this method, called Gaussian Frequency Shift Keying (GFSK). EDR was introduced in Bluetooth 2.0, and High Speed (HS), also known as "Alternative MAC/PHY" (AMP), was introduced in Bluetooth 3.0 [67]. The modulation mechanism used by EDR is Differential Phase Shift Keying (DPSK). Piconet and Scatternet are two different forms of Bluetooth communication typologies. Piconet is a collection of ad hoc connections among Bluetooth-enabled devices. A piconet begins with two connected devices and can expand to eight, one master, seven active slaves, and 255 parked slaves. A piconet is an architecture based on stars topology, in which the slave communicates only with the master, as shown in Figure 7. Figure 8 represents coexisting piconets, with each piconet utilizing the frequency sequence determined by the master [68].

Bluetooth Special Interest Group (SIG) introduced BLE in version 4.0. It was designed for a low-power wireless network that does not need high throughput and for use in scenarios where Bluetooth was not traditionally appropriate. The link layer, PHY layer, and packet formats were remodeled to obtain lower energy consumption. Furthermore, BR/EDR is only intended for two-way communication [69]. Due to its accessibility in smartphone devices, its low cost, and power consumption, BLE technology has evolved into an effective alternative. It is completely IoT-ready [70,71].

Table 1 represents the two major categories of Bluetooth technology: Bluetooth classic refers to older Bluetooth versions, primarily intended for file transmission and audio streaming, and BLE, which refers to newer Bluetooth versions for IoT applications with low power usage. Both BLE and BR/EDR are becoming more popular as consumers desire low power and high throughput. BLE makes use of 37 general purpose physical channels, as well as three advertising channels. In various applications, one of the shortcomings of the initial version of Bluetooth was that the data rate was insufficient relative to many other wireless protocols, such as 802.11. However, the Bluetooth wireless communication standard has been updated to version 5.0, doubling the previous version's transmission rate [72]. BLE 4.2 and BLE 5 have data speeds of 1 kbps and 2 kbps, respectively. On the other hand, a BLE system would have substantially lower throughput. It must take into consideration a variety of protocol overheads, as well as adaptive RF connection changes to preserve reliable links in the presence of noise. Protocol restrictions, depending on

BLE data transfer processes and strategies, such as connectivity duration, frame size, and acknowledgement technique, are also required.

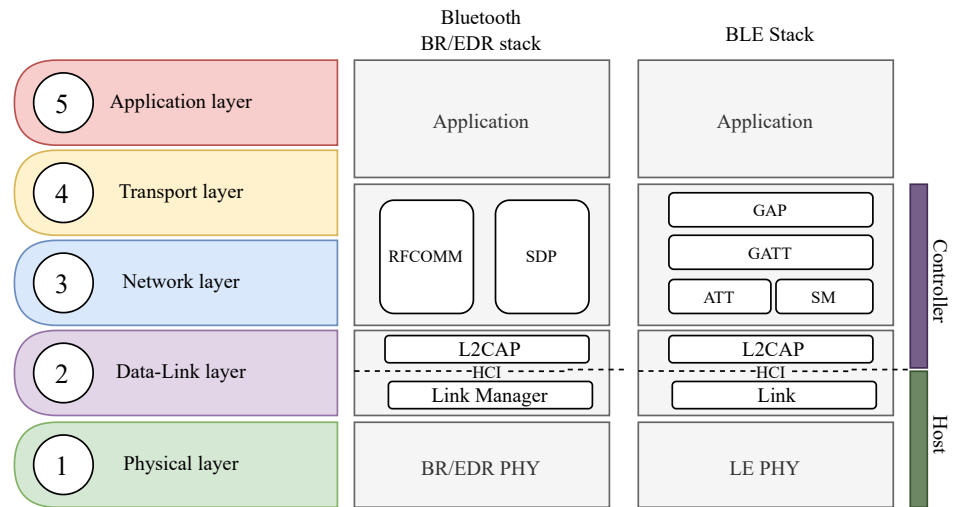


Figure 6. Comparing Bluetooth BR/EDR and BLE stacks with OSI stack.

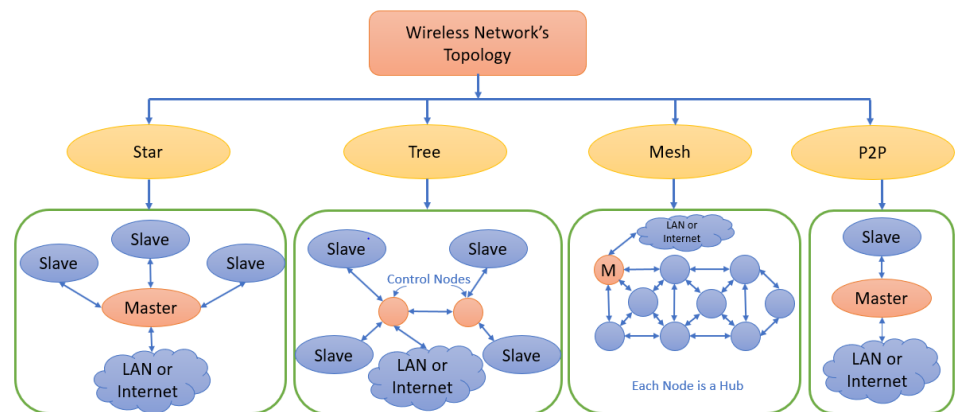


Figure 7. Different network topologies.

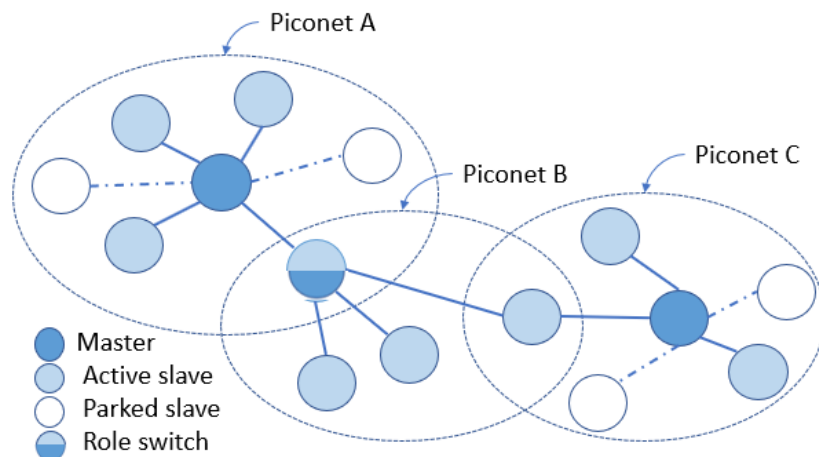


Figure 8. An example of a Bluetooth Scatternet.

Table 1. Comparison of Bluetooth versions.

Specifications	Bluetooth Classic BR/EDR	BLE	
		Bluetooth 4.x	Bluetooth 5
Radio freq. (MHz)	2400 to 2483.5	2400 to 2483.5	2400 to 2483.5
Channels	79 (1 MHz)	40 (2 MHz)	40 (2 MHz)
Distance (m)	Up to 100	Up to 100	Up to 200
Latency (ms)	100	<6	<6
Data rate (Mbps)	1, 2, 3	1	0.5, 0.125, 1, 2
Max active nodes	8	Unlimited	
Message size (bytes)	Up to 358	31	255
Max payload (bytes)	1021	37,255	255
Peak current (mA)	<30	<15	<15

5.2.1. BLE Mesh

In its early stages, BLE was designed around a star topology, where the master module was at the network's epicenter, and the slaves were at its periphery. Therefore, the master was the only point of contact for all messages. In 2017, Bluetooth SIG announced that mesh topology is supported with Bluetooth standard 5.0. This transformation has led to the development of several mesh network mechanisms, and, consequently, to the classification of the various types of BLE mesh networks [73]. Bluetooth mesh networking provides many-to-many (m:m) device connections. Most BLE mesh protocols are built as layers on top of a standard Bluetooth star network. The networking can be used in a variety of industries, such as the smart building industry, notably in commercial lighting systems and sensor network solutions in various applications. In addition, it is suitable for large-scale device networks and IoT technologies with multiple devices communicating with each other. This BLE stack was modified to support encrypting and authenticating all mesh messages using provisioning data and the application key, and relaying them. It is also responsible for segmenting and reassembling mesh communications as needed. Therefore, the Mesh topology of Bluetooth is highly profitable for smart homes/offices and industrial controls. Although ZigBee is perfect for home automation, Bluetooth may eventually take over because Bluetooth is available on all computers and mobile phones, making it simple for users to operate so as to manage their home offices using their smart devices.

5.2.2. Beacon Technology (iBeacon)

The advancement of either Near Field Communication (NFC) or Quick Response (QR) code technology led to iBeacon technology. An iBeacon is a tiny device that uses BLE to frequently transmit specific data across a predetermined area. It may be operated for a maximum of two years by a coin cell due to BLE's low energy consumption. However, the transmission output power (TX power) and advertisement period selections impact battery lifetime. Beacons have a maximum range of 70 m. Nevertheless, this may be significantly diminished according to surrounding obstacles. Estimote, Kontakt, Gimbal, and other vendors produce BLE beacons. A beacon comprises a Bluetooth chipset (including firmware), a power supply battery, and an antenna. The main BLE chips' current producers are Texas Instruments, Nordic Semiconductor, Bluegiga, and Qualcomm.

5.3. Z-Wave

Z-Wave is a newer version of RF that is cheap, has low energy consumption, is accurate, and is applicable for small-distance wireless communication systems [74]. It was originally developed by a Danish company, called Zensys, based in Copenhagen in 1999 [75]. It is a patented technology that merges sensors and actuators over RF to provide smart home and office automation services. Although the protocol is publicly disclosed, details about

the network layer are still not ready for analysis. The Z-Wave routing protocol’s frame forwarding and topological management aspects are reverse-engineered using a real-world Z-Wave network [76]. It mainly uses strong AES 128-bit encryption for securing connected devices. A Z-Wave network can handle up to 232 devices or up to 4000 nodes on a single network [77].

As shown in Figure 9, Z-Wave is a reduced MAC protocol commonly used in home automation systems. Other than home automation, it is used in various other IoT applications. It has a range of up to 100 m, allows point-to-point communication, and is ideal for sending short messages. It employs CSMA/CA for accurate communication systems, including a small acknowledgment message. A Master and slave system comprises the Z-Wave infrastructure. The Master manages the network’s scheduling and commands all slaves linked to it [78].

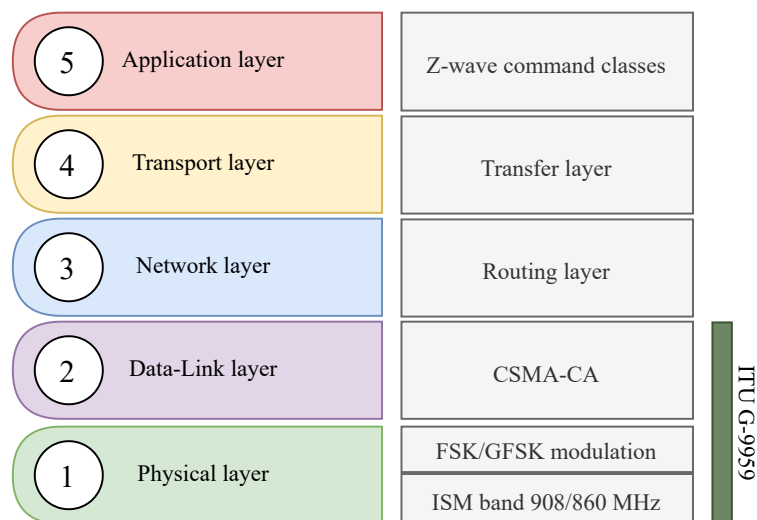


Figure 9. Comparing Z-wave stack with OSI stack.

5.4. Wi-Fi

Wi-Fi is a subset of the IEEE 802.11 protocol family that enables users to establish wireless connections to the Internet. It is a perfect option for many IoT applications, since its utility is well-known and widely available, including in people’s homes, workplaces, and other locations [61]. It utilizes various encryption protocols for security purposes, which are Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), and Wi-Fi Protected Access Version 2 (WPA2) [79]. The IEEE 802.11 is a set of protocols for wireless LANs (WLANs). It has evolved through multiple generations: 802.11b, 802.11a, 802.11g, 802.11n, 802.11ac, 802.11ah, 802.11ax, and, finally, the 802.11be. The Wi-Fi Alliance adopted a new name strategy for the 802.11 protocols in 2018 to make them easier to memorize. Table 2 compares the old and updated naming conventions, along with the features of each one and the utilized technologies. The range of possible data rates offered by these specifications is 11 kbps to 40 kbps. The communication range of Wi-Fi is roughly between 20 m (indoors) and 240 m (outdoors) [80].

Among these amendments, the IEEE 802.11ah (Wi-Fi HaLow) is a solution that enables better power consumption, better coverage quality of service, scalability, and affordability for a variety of IoT applications. Wi-Fi HaLow is one of the Low-Power Wide Area Network (LPWAN) technologies that operate at frequencies below 1 GHz [81]. It was developed to connect large numbers of IoT and M2M gadgets [82]. However, the security features of 802.11ah have a significant implementation problem in meeting the requirements of resource-limited IoT nodes [83]. Although Wi-Fi HaLow was designed to facilitate long-distance connectivity while using less energy, it still suffers from high power consumption when compared to other IoT protocols like BLE and ZigBee. Wi-Fi has advanced to its sixth generation with the release of IEEE 802.11ax, which outperforms its predecessor,

802.11ac [84]. Unlike the previous amendments, Wi-Fi 6 includes numerous significant wireless advances that are especially useful for IoT applications. The adoption of 2.4 GHz is the first major modification. Unfortunately, Wi-Fi 5 can only operate at 5 GHz. The 5 GHz range has less interference of RF; however, it has worse wall penetration and longer battery drain than 2.4 GHz offers. The 2.4 GHz frequency remains the preferred frequency for Wi-Fi-powered IoT devices. The usage of Orthogonal Frequency Division Multiple Access (OFDMA) and Multi-User, Multiple-Input, Multiple-Output (MU-MIMO) is another key distinction between the two specifications, which expands the range of IEEE 802.11ac's multi-user (MU) communication. Wi-Fi 6 supports both downlink and uplink MU-MIMO, while Wi-Fi 5 only supports downlink [85]. Similarly to how OFDMA is exclusive to Wi-Fi 6, this feature is only accessible via that standard [86]. MU was developed to accommodate a high number of interconnected devices while maintaining a minimal collision rate and access time, and it permits numerous synchronous transmissions from various sites. On the other hand, the next Wi-Fi 7 update will provide new capabilities for time-sensitive networking (TSN) [87]. High quality of service (QoS) applications, such as remote healthcare monitors and robotic management, will be supported by this version thanks to the new suggested features [88]. Wi-Fi 6 adopted OFDMA to increase spectrum effectiveness and enable large-scale operations, but Wi-Fi 7 is anticipated to further optimize OFDMA efficiency with the inclusion of additional characteristics to the OFDMA process [89]. Allocating spectrum resources employing an access point (AP) for scheduling may have an impact on the latency. When it obtains the transmission opportunity (TXOP) frame, the AP works as a scheduler and requests uplink transmission from the stations. As a result, use of an optimum scheduling strategy is necessary to get the best delay performance [90]. The definition of a low-latency access category (LL-AC) has the potential to provide reliable operation at a predetermined latency [91]. This will be extremely beneficial for a wide range of latency-sensitive applications, including gesture recognition, object control tracking, healthcare monitoring, and other industrial IoT applications [92].

5.5. 6LoWPAN

In 2007, the IETF working group developed the 6LoWPAN protocol [93]. Using IEEE 802.15.4 standard radios, 6LoWPAN provides operation in the 2.4 GHz ISM band across the globe, at 913 MHz in North America and 868 MHz in Europe. The signal range is up to 100 m, and the highest data rate is 250 kbps [94]. The group has specified encapsulation and header compression algorithms to send and receive IPv6 packets over IEEE 802.15.4-based networks, as shown in Figure 10. This reduces the IPv6 header size from 40 bytes to 7 bytes. 6LoWPAN uses a self-healing, time-synchronized, and self-organizing mesh architecture [57]. Furthermore, 6LoWPAN integrates the most recent generation of the Internet Protocol (IPv6) with LowPAN networks, allowing low-powered devices to communicate remotely over short distances [95]. Therefore, it is necessary to implement an adaptation layer employing header compression to transmit IPv6 packets across IEEE 802.15.4 networks efficiently. Furthermore, because most of the routing methods used on standard IPv6 networks are incompatible with the limited networks that 6LoWPAN operates on, a new routing protocol, called IPv6 Routing Protocol for Low Power and Lossy Networks (RPL), was explicitly created for 6LoWPAN [93]. RPL is a popular routing protocol due to its flexibility, energy-efficient routing capacity, and QoS support [96]. It is based on source and distance vector routing protocols. Point-to-point, point-to-multi-point, and multi-point-to-point topologies are all supported by RPL. RPL assembles nodes into a Destination Oriented Directed Acyclic Graph (DODAG) topological structure [97]. Each user receives an IP address in the range of 5:1028, and these addresses are distributed independently to each device using the 6LoWPAN protocol. Regarding security, 6LoWPAN utilizes the strong AES-128 link-layer security mechanisms introduced by IEEE 802.15.4. A typical 6LoWPAN device may have an average current consumption of a few tens of microamperes (μA) during normal operation and a sleep current consumption of a few

nanoamperes (nA) when the device is in a low-power sleep mode [98]. Applications of 6LoWPAN include automation, industrial monitoring, smart grid, and smart home.

Table 2. Summary of the different features of 802.11 family amendments.

Amendment	Naming Convention	Year	Operating Band	Max Bandwidth	Max Data Rate	PHY	MAC
802.11b	Wi-Fi 1	1999	5 GHz	22 MHz	11 Mbps	DSSS	DCF ¹
802.11a	Wi-Fi 2	1999	2.4 GHz	20 MHz	54 Mbps	OFDM	DCF
802.11g	Wi-Fi 3	2003	2.4 GHz	20 MHz	54 Mbps	MIMO-OFDM	DCF
802.11n	Wi-Fi 4	2008	2.4/5 GHz	40 MHz	600 Mbps	OFDM	DCF + EDCA ² , frame aggregation, BA ³
802.11ac	Wi-Fi 5	2014	5 GHz	40 MHz	6.39 Gbps	256-QAM, OFDM, DL MIMO, channel bounding	DCF + EDCA, frame aggregation, BA
802.11ah	Wi-Fi HaLow	2017	sub-1 GHz	16 MHz	347 Mbps	OFDM, DL-MU MIMO	EDCA, TWT, RAW ⁴
802.11ax	Wi-Fi 6	2019 2020 (6E)	2.4/5 GHz, 6 GHz for Wi-Fi 6E	160 MHz	9.6 Gbps	OFDMA, UL/DL MIMO, channel bounding	DCF + EDCA, frame aggregation, BA, TWT ⁵ , MU channel access
802.11be	Wi-Fi 7	2024	2.4/5/6 GHz	320 MHz	40 Gbps	4096-QAM, Coordinated OFDMA, UL/DL MIMO	HARQ ⁶ multi-link aggregation, Multi link operation, ...

¹ Distributed Coordination Function; ² Enhanced Distributed Channel Access; ³ Block Acknowledge; ⁴ Restricted Access Window; ⁵ Target Wake Time; ⁶ Hybrid Automatic Repeat Request.

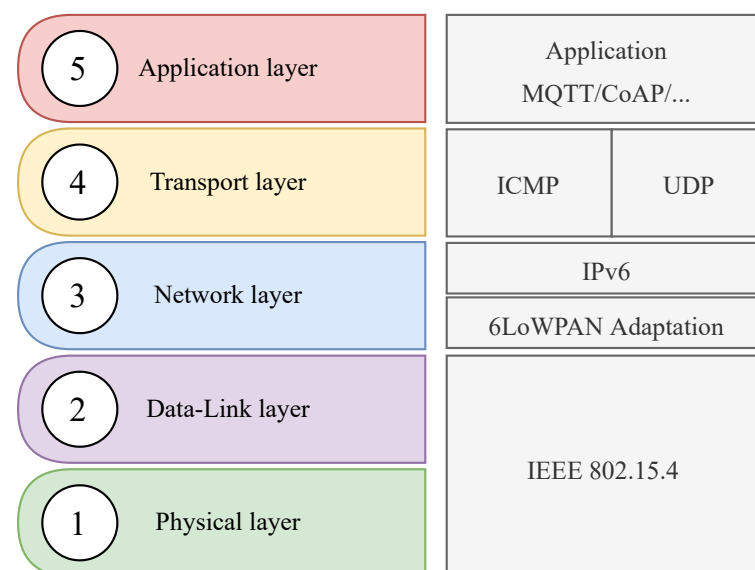


Figure 10. Comparing 6LoWPAN stack with OSI stack.

5.6. Wi-SUN

The Wireless Smart Utility Network (Wi-SUN) protocol was developed in 2012 and became an open standard, based on IEEE 802.15.4g [95]. The Wi-SUN is a mesh networking protocol that supports bidirectional communication and operates in the 800 MHz, 900 MHz, and 2.4 GHz frequency bands according to the region. The Wi-SUN is made up of a border router that connects the mesh network and the backhaul network, and Wi-SUN end-nodes [99]. Owing to its effectiveness in header compression, 6LoWPAN is integrated into the Wi-SUN profile, so Wi-SUN provides complete IP packets with header compressing to minimize bandwidth. Therefore, long-range connectivity is assured, and the battery lifespan is extended. The Wi-SUN has a power consumption of less than 2 μ A (resting) and 8 mA (listening). It has data rates of up to 300 kbps and latency in the tens of milliseconds range [100]. It supports multiple modulation techniques for wireless communication, including OFDM and DSSS. The Wi-SUN connectivity schemes are classified into three types. [101]. Category “1” is a wide-area open space information sensing and monitoring system. This category is based on fixed point-to-multipoint communication and has a 1–5 km range. Category “2” is a wide-area urban information sensing and monitoring system. In this category, multi-hop operation between radio devices or via Wi-SUN routers may be used. Category “3” is a wide area mobile communication information sensing and monitoring system. The Wi-SUN technology offers a set of stacks, also known as profiles, that are optimized for certain uses [102]. The profiles created by the working groups (WGs) in the Wi-SUN alliance are summarized in Figure 11. The standards are currently developed by the Home Area Network (HAN) WG, Field Area Network (FAN) WG, Resource-Limited Monitoring and Management (RLMM) WG, and Japan Utility Telemetry Association (JUTA) WG. Many applications utilize the Wi-SUN protocol, such as asset management, environmental monitoring, agriculture, and structural health monitoring [103].

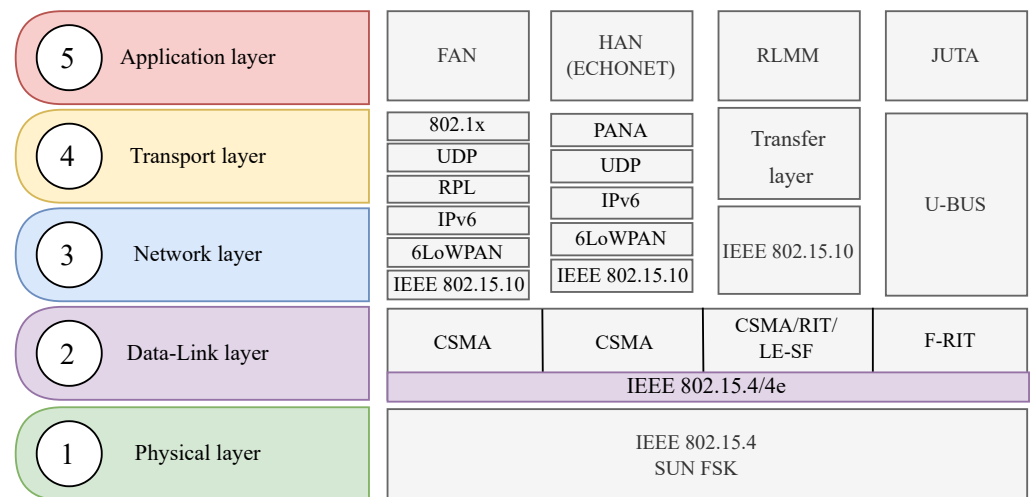


Figure 11. Comparing Wi-SUN different profiles with OSI stack.

5.7. LoRa

LoRa wireless technology sends low-power data packets over a long distance to another receiver node [104]. It originated in 2009 when two friends, Nicolas Sornin and Olivier Seller, from France decided to create a low-power, long-range modulation method. The LoRa architecture employs a network server, an application server, a gateway that manages numerous devices simultaneously [105], and other components, a majority having different wireless communication designs, as shown in Figure 12. According to the LoRa Alliance, LoRa wireless technology uses the LoRaWAN protocol designed for battery-operated wireless devices. The LoRaWAN network architecture can be implemented as a star topology with bidirectional communication between end nodes and gateways. Its modulation technique is derived from Chirp Spread Spectrum (CSS) technology, as it uses

chirp pulses to encode information over radio waves. LoRa provides up to three miles (five kilometers) of coverage in urban regions, and up to ten miles (15 km) or more (line of sight) in rural areas [106]. It supports mutual authentication, integrity protection, and confidentiality. It mainly relies on the standardized AES cryptographic algorithm. The applications of LoRa include smart agriculture, industrial internet of things, smart supply chain, smart environment, and smart buildings [107].

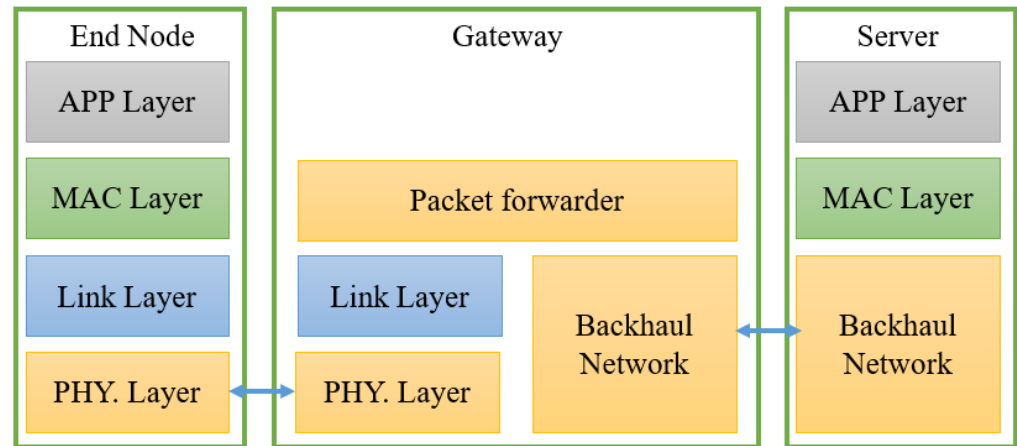


Figure 12. LoRa network stack.

5.8. LoRaWAN

The LoRa Alliance, which was founded in February 2015, created a layer on top of LoRa technology called LoRaWAN. It establishes functionalities for communication [108] (shown in Figure 13). LoRaWAN is one of the most widely-used low-power wireless technologies for communication over long distances featuring low data rates. LoRaWAN is ideal for sending small payloads, such as sensor data, over long distances. This offers a substantially longer communication range while maintaining low bandwidths, compared with other wireless data transmission technologies [109]. It also provides a coverage distance of up to 25 miles in line-of-sight or 800 m through buildings. It mainly utilizes the Advanced Encryption Standard (AES) 128-bit symmetric encryption as a security technique. Many applications utilize the LoRaWAN protocol, such as smart agriculture, smart city, and smart industrial control [110].

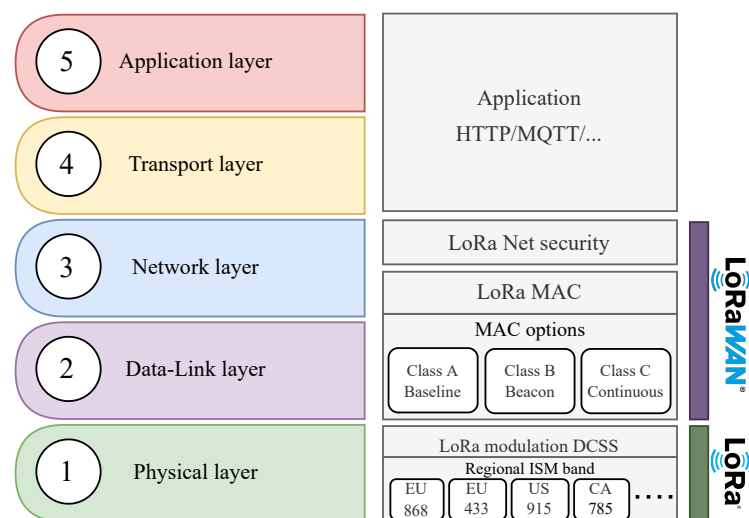


Figure 13. Comparing LoRaWAN stack with OSI stack.

5.9. NB-IoT

Narrow-Band IoT is a mobile communications protocol with a bandwidth of 180 kHz that the 3GPP standardization group specifically standardized in 2016 [111]. With each 3GPP version, NB-IoT improved in support for more data rate, higher network capacity, better power utilization, better compatibility with 5G New Radio (NR), and more. In 2022, Release-17 was standardized introducing 16-QAM in UL/DL, as well as support for up to 14 HARQ processes. NB-IoT is increasingly being used to support machine-type 5G and Long-Term Evolution (LTE) [112] communication by establishing other ultra-low IoT devices that benefit from enhanced coverage, deep penetration, deployment flexibility, and lower energy consumption. In addition, the variety of LTE networks' frequency bands can provide flexibility in deployment options [113]. NB-IoT has 3 distinct operational modes. The narrowband is used inside an LTE carrier while operating in the in-band option. The Guardband mode allows NB-IoT to take advantage of LTE's spare bandwidth. In the standalone configuration, the narrowband is used in its frequency band [114]. In all deployment modes, NB-IoT offers strong penetrating power and the best coupling loss performance. The NB-enhanced IoT's indoor coverage, reduced latency, sensitivity, ultra-cheap device cost, minimal power consumption, and inherited LTE security are other remarkable features [115]. NB-IoT supports Standalone (SA), Guard-band (GB), In-band (IB), and Hybrid topologies [116]. In SA topology, NB-IoT operates as a standalone network without any interconnection to existing cellular networks. It is suitable for deployment in remote or rural areas where no existing cellular infrastructure is available. In GB topology, NB-IoT operates in the guard band of the existing cellular networks, using the unused spectrum between the DL and UL frequency bands. It allows NB-IoT to coexist with existing cellular networks and reuse the existing infrastructure, making it cost-effective. In IB topology, NB-IoT operates in the same frequency band as the existing cellular networks, sharing the same infrastructure. It is suitable for deployments in urban areas where the existing cellular networks have high capacity and coverage. In Hybrid topology, NB-IoT can operate in both the guard band and in-band modes simultaneously, allowing for more flexibility in network deployment. It has a coverage distance of approximately 1km in urban areas and 10km in rural areas. Common applications which utilize NB-IoT are, for example, smart metering, smart buildings, and smart parking solutions. The network structure of NB-IoT is based on five components: terminal, base station, core network, cloud platform, and vertical business center [117]. These components are shown in Figure 14.

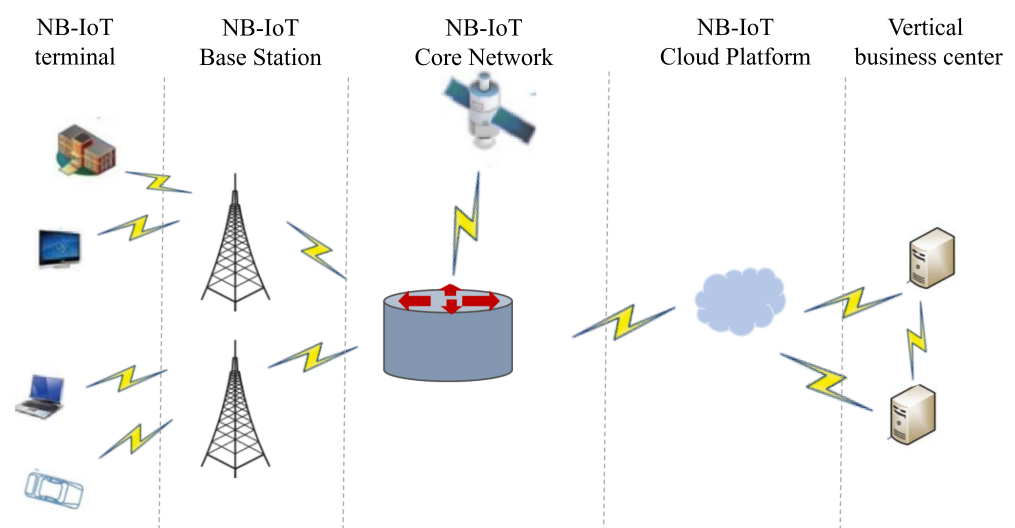


Figure 14. NB-IoT network structure.

5.10. Wired Communication Protocols

5.10.1. PLC

The PLC protocol uses power transmission lines to send data [118]. It originally emerged in 1838 when a remote measurement system was initially introduced for monitoring the battery levels of sites far from a telegraph system. The PLC operates at a frequency of 300–500 kHz, with a data rate of up to 10–500 kbps and up to 3 km. It is ideal for smart grid communication in highly populated locations since it has a high throughput and low latency. It can be employed in practically every aspect of a smart grid environment, from low-voltage residential appliances to high-voltage grid control [119]. It utilizes the AES and DES cryptographic mechanisms for security purposes. According to the current transferred by the electric wires, PLCs can be categorized into PLC over AC (Alternative Current) or PLC over DC (Direct Current) [120]. In PLC networks, the modem node modulates the supplied data before injecting it into the transmission medium and sending it to its target. [121]. The modulation methods that may be used with this system are spread-FSK, binary phase-shift keying (BPSK), OFDM, and FSK [122]. The PLCs have been used in a variety of domains, such as narrow-band PLC radio broadcasting, networking, and transportation [123]. The PLC has three main categories; Narrowband PLC, Mid-band PLC, and Broadband PLC. Narrowband PLC (NB-PLC) has a frequency of less than 148.5 kHz European (EU) and less than 4920 kHz Federal Communications Commission (FCC). It has a low rate and massive communication of up to 1000, and a transmission distance of more than 1 km. It is used in low-voltage power distribution network automation and meter reading. Mid-band PLC has a frequency of 0.7 to 12 MHz. It has low latency and high reliability of up to 99.99%. It is used in smart traffic lights and smart meters. Broadband has a frequency of 1.8 to 30 MHz and 1.8 to 100 MHz. It has a large bandwidth with a latency of less than 50 ms and a transmission distance of fewer than 200 m. It is used in home broadband access and interconnection [124]. Table 3 illustrates that some alliances have produced prominent standards for NB-PLC, such as Powerline Intelligent Metering Evolution (PRIME) (ITU-T G.9904), G3 PLC (ITU-T G.9903), IEEE 1901.2–2013, and ITU-T.G.hnem [125]. G3-PLC and PRIME are open and have been adopted as starting points for the official ITU standard, G 9955 Narrow-band OFDM-based PLC transceivers PHY specification [126].

Table 3. NB PLC Standards.

Standard	Data Rate	Frequency Range
X-10	-	95–125 kHz
KONNEX EN50056-1	1.2–2.4 kbps	125–140 kHz
IEC61334	2.4 kbps	3–95 kHz
ISO/IEC 14,908–1	3.6–5.4 Kpbs	86–131 kHz
G3-PLC	5.6–46 kbps	3–490 kHz
PRIME	130 Kpbs	3–95 kHz
IEEE P1901.2	500 kbps	9–500 kHz
ITU-T G.hnem	1 Mpbs	up to 500 kHz

PRIME: PLC technology called PRIME is based on the ITU G.9904 specification. It takes advantage of already-existing medium and low-voltage power distribution networks to efficiently connect the components of a smart grid through the use of OFDM technology. The PRIME Alliance created PRIME technology, which the ITU has designated as an international standard. Version 1.4 of PRIME is an improvement over version 1.3. (v.1.3). The PHY and MAC updates are part of PRIME version 1.4. These changes have enabled several enhancements, including increased resilience, faster data transfer rates, expanded

capacity, more band planning flexibility, and IPv6 capability for the convergence layer. Additionally, these innovations are compatible with PRIME v1.3 products already on the market. G3-PLC: The G3-PLC Alliance created an SG-oriented communication protocol that includes the PHY, MAC, and 6LoWPAN network layers. With a high data rate, high-speed, and long-range communication capacity over the current power-line grid, the G3-PLC standard can also cross distribution-transformers [127].

5.10.2. Ethernet

Ethernet was created to provide link-layer communication via packet switching. It was originally developed by Bob Metcalfe at the Xerox Palo Alto Research Center in 1973 and initially supported by thick copper coaxial-type cables. It is commonly used in connecting devices within local area networks and provides communication of up to 100 m. Its modulation technique is based on Pulse Amplitude Modulation (PAM) and supports both bus and star topologies [128]. It translates datagrams from the top network layer into frames for transmission across wireline networks. The IEEE 802.3 standard governs Ethernet, which allows for nominal transfer rates of up to 400 kbps. Ethernet is divided into numerous wiring and signaling versions of the OSI physical and data connection layers [129]. Regarding power consumption, it varies depending on many factors, such as Ethernet type, standard used, cable length, and involved device power efficiency. The 10BASE-T and 100BASE-T standards typically consume less than 5 Watts per port, while newer standards, such as 1000BASE-T and 10GBASE-T, may consume up to 15 Watts or more per port [130].

5.11. Hybrid Technology

G3-PLC Hybrid PLC and RF Profile

The G3 Alliance specification-based G3-PLC systems have been utilized in several Advanced Metering Infrastructure (AMI) and smart grid deployments across numerous nations worldwide. In 2020, the G3-PLC Alliance decided to start work on defining the G3-PLC Hybrid PLC and RF profile to expand G3-PLC’s versatility and relevance on global markets [131]. The new hybrid protocol stack combines the primary G3-PLC media with a supplementary channel made up of PHY and MAC RF lower layers depending on IEEE 802.15.4 and IEEE 802.15.4v Smart Utility Network (SUN) FSK RF technologies, as shown in Figure 15. The first version of the G3-PLC Alliance hybrid companion standards supports the spectrum range 863–870 MHz. Additionally, the adaptation layer uses the Lightweight On-demand Ad hoc Distance-vector Routing Protocol – Next Generation (LOADng) routing scheme to determine the transition between primary (PLC) and secondary (RF) media [132].

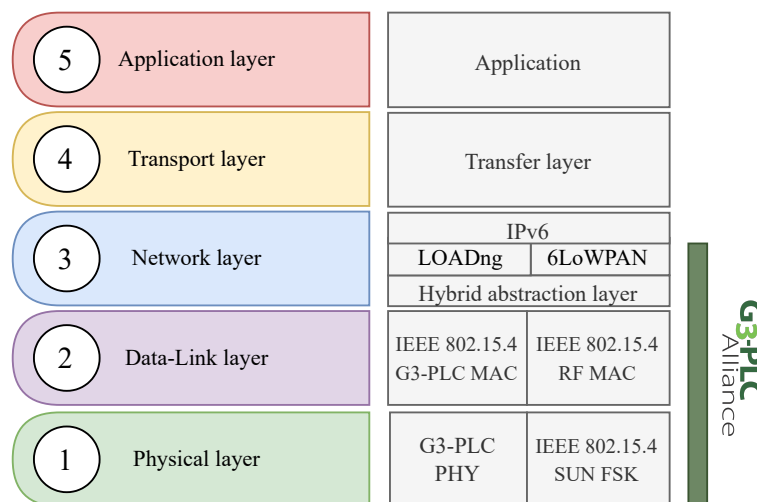


Figure 15. G3-PLC Hybrid PLC and RF protocol stack.

By providing suitable interfaces, the hybrid abstraction layer links the 6LoWPAN adaptation layer to the dual lower layer stacks. This increases the overall reliability of the hybrid protocol stack by enabling communication via the alternative media if the specified channel is identified in the routing table but fails during transmission [132]. The LOADng routing protocol is a mechanism for assessing connection costs over RF networks, generating optimum routes depending on the routing metric and keeping them up to date.

6. IoT Hardware Platforms

The power of IoT and computing abilities are reflected by the processing elements, such as microcontrollers (MCUs), systems-on-chip (SoC), systems-in-package (SiP), and field programmable gate arrays (FPGAs). There are many different educational and evaluation boards available for running IoT applications, including Arduino, Raspberry PI, UDOO, Intel Galileo, FriendlyARM, BeagleBone, Gadgeteer, and T-Mote Sky. The IoT is also implemented using a wide range of devices and computerized systems. SoC and SiP technologies are often used to create semiconductor options for IoT devices. While the SoC technique enables semiconductor processes to combine analog, digital, mixed-signal, and RF circuitry on a chip, SiP technology uses packaging processes to combine functional elements created independently into a package, including MCUs, oscillators, and even antennas. By using SoC technology, we may increase system stability and usability while greatly decreasing overall system expenses. However, there are tradeoffs in device performance and energy usage. The SiP devices, on the other hand, boost unit speed and improve power utilization at the expense of reduced reliability and greater system cost, due to the usage of a variety of materials and procedures in the fabrication of the functional units included inside the packages [133]. Table 4 compares various industrial IoT-compliant SoCs and SiPs from different vendors. Each hardware module supports one or many wireless communication technologies. On the other hand, firmware is crucial to computational platforms since it controls the execution of a device throughout its life cycle [134]. Some IoT applications may be improved with the help of Real-Time Operating Systems (RTOSs) [135]. For instance, the Contiki RTOS has seen extensive use in IoT applications. Other embedded IoT solution providers include TinyOS, RiotOS, and LiteOS [136]. One other essential computational area for the IoT is cloud platforms. These solutions advocate for the use of connected devices for data transmission to the Internet, for the periodic analysis of big data sets, and for end-users to reap the most benefit possible from the insights gained from the analysis of this data. The cloud platforms and accessible sites to deploy IoT services are many, and a lot of them are provided at no cost and geared toward commercial use.

Table 4. Comparison of industrial IoT-compliant devices from different vendors.

Vendor	Hardware Model	Supported Wireless Technologies	Sensitivity [dBm]	Transmit Current [mA]	Receive Current [mA]
Texas Instruments	CC2651R3SIPA	BLE, 802.15.4	−104	7.1	6.8
Texas Instruments	CC2652PSIP	BLE, 802.15.4	−103	7.9	7.3
Texas Instruments	CC2651P3	BLE, 802.15.4	−104	7.1	6.4
Texas Instruments	CC2652RSIP	BLE, 802.15.4	−99	7.5	7.3
Nordic	nRF5340	BLE 5.3, 802.15.4	−98	3.4	2.7
Nordic	nRF52840	BLE 5.3, 802.15.4	−103 for BLE 5.3, −100 for 802.15.4	6.40	6.26
NXP	K32W041AM-A	BLE, 802.15.4	100	12.1	4.3
Infineon	CYW20736S	BLE (SiP)	−94	24–28	24–28
STMicroelectronics	STM32WB30CE	802.15.4	−100	8.8	7.9
STMicroelectronics	STM32WB35CC	802.15.4	−100	5.2	4.5
Texas Instruments	CC3230S	802.11b/g/n	−96 dBm at 1 DSSS, −74.5 dBm at 54 OFDM	223	59

Table 4. Cont.

Vendor	Hardware Model	Supported Wireless Technologies	Sensitivity [dBm]	Transmit Current [mA]	Receive Current [mA]
Texas Instruments	CC3235MODAS	802.11a/b/g/n	−94.5 dBm at 1 DSSS, −89 dBm at 6 OFDM	223	59
Texas Instruments	CC1352P7	Wi-SUN	−121	21 at +10 dBm at 2.4 GHz	6.4 at 2.4 GHz
Texas Instruments	CC1312R7	Wi-SUN, 6LoWPAN	−121	24.9 TX at +14 dBm at 868 MHz	5.4 RX at 868 MHz
Texas Instruments	CC1352X	Wi-SUN, 6LoWPAN, BLE 5.2, ZigBee	−121	8.0 at 868 MHz	5.8 at 868 MHz)
STMicroelectronics	SPIRIT1	6LoWPAN	−120	54	9
ROHM Semiconductor	BP35C0-J11	Wi-SUN	−103	47	27
STMicroelectronics	S2-LP	Wi-SUN, 6LoWPAN	−130	10	7
Nordic	nRF9160	LTE, NB-IoT	−114	0.009	–
STMicroelectronics	ST87M01	NB-IoT	N/A	N/A	N/A
Silicon Labs	ZGM130S	Z-Wave	−103.9 dBm	13.3 at 0 dBm	9.8
Silicon Labs	ZGM230S	Z-Wave	−109.8 dBm	10.7 at 0 dBm	4.1
Microchip	PL360	PLC	N/A	N/A	N/A
Renesas	R9A06G037	PLC	N/A	N/A	N/A
Renesas	PL3120	PLC	N/A	N/A	N/A
STMicroelectronics	STM32WL54CC	LoRaWAN	−148	15 at 10 dBm	4.82
STMicroelectronics	STM32WL54JC	LoRaWAN	−148	15 at 10 dBm	4.82

7. IoT Simulation Tools

Due to increasing attention in regard to IoT and WSNs, modern simulators are becoming more and more widespread [137]. Selecting a reliable simulator is a challenging and long-lasting endeavor, particularly in the WSNs arena, where several complicated situations and various protocols need network simulators with specific functionality. Many WSN simulators, including OpenDSS, Network Simulator-2 (NS-2), NS-3, OMNET++, GridLab-D, and GloMoSim, are created to support the simulation operation of IoT setups.

7.1. OpenDSS

OpenDSS is a distributed simulation software that is free to use. OpenDSS was created as an open-source power system simulator for the electric distribution system by Microsoft [138]. General AC circuit analyzer, Annual load generation simulation, Wind-power simulation, Annual power flow simulation, and Annual load generation simulation are all supported by it. In addition, the simulation aids in handling fault analyses [138].

7.2. NS-2/NS-3

NS-2 is a network simulator that is free to use that simulates communication protocols and network topologies. Both wireless and wired networks are supported. Users can play, pause, forward, and stop the simulation using the network animator. However, it is not a real-time simulation termed a virtual world [139]. NS-3 is an enhanced version of NS-2, not a successor. NS-3 supports both parallel and emulation simulation [140].

7.3. OMNET++

OMNET++ is a free and open-source simulator that supports Mac OS, Windows, and UNIX. OMNET++ consists of the unit and simple modules that emphasize the model's atomicity, allowing multiple unit modules to be integrated to create a complex module [141].

These unit modules are written in C++, but NETwork Description (NED) is responsible for integrating them into a network simulator setup. This tool covers a wide range of areas, including ad-hoc networks, peer-to-peer networks, IPv6 networks, sensor networks, storage area networks, and wireless networks [142].

7.4. GridLab-D

GridLab-D employs end-use models, such as the consumer, equipment and application, operations and business simulation tools, retail market models, agent-based modeling methodologies, and SynerGEE’s power distribution model [143]. In addition, it can incorporate third-party analysis software and data management [144].

7.5. MATLAB/Simulink

MATrix LABoratory (MATLAB), developed by MathWorks, comes with a visual interface. Simulink is the name of the interface [145]. It provides many capabilities; Algorithm Development, Graphics, Application Building, Parallel Computing, and Data Analysis [146].

7.6. GloMoSiM

The Global Mobile Information System Simulator is written in Parsec and C and is primarily used for parallel programming software. It supports a wireless satellite communication system that supports thousands of nodes with heterogeneous connectivity. In addition, it includes a simulation library and a parsec compiler [147]. Figure 16 compares various IoT simulators based on IoT criteria and features with justifications provided for each chosen criterion, including availability, which represents if the simulation tools are open-sourced or licensed, description of the simulator’s programming language and how easily future hardware models will be able to utilize the simulated primitives. This most significant network scale can be offered and simulated through simulator tests if the simulator supports the emulator.

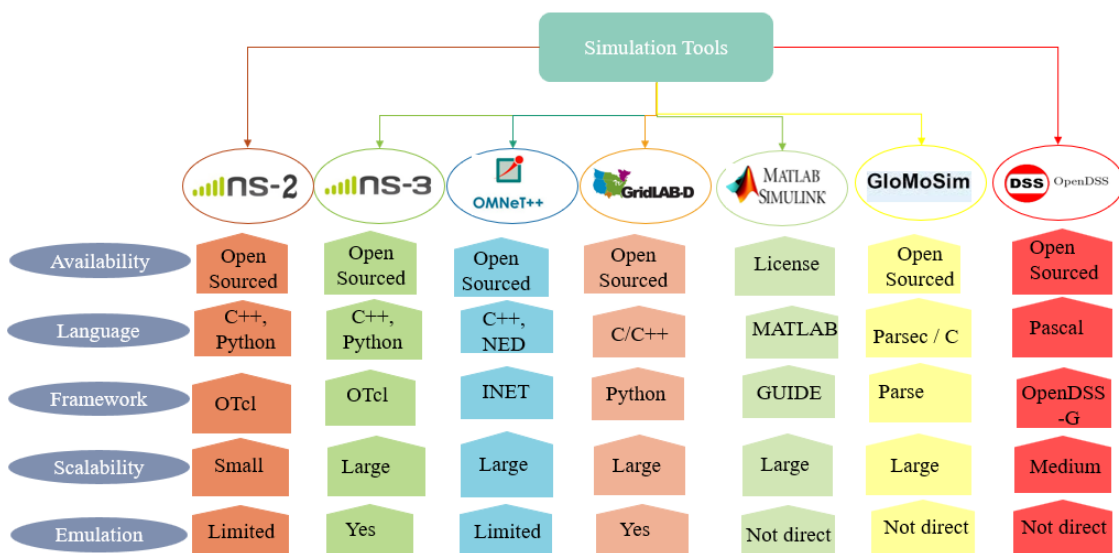


Figure 16. Simulation Tools.

8. IoT Challenges

Despite the advantages of IoT when it comes to many applications, such as Agriculture 4.0, Industry 4.0, and wearable devices, IoT faces various challenges [148]. In this section, we discuss the IoT challenges in multiple aspects, such as standardization, scalability, heterogeneity, interoperability, availability of services, power consumption, and environmental concerns.

Standardization of the IoT is considered one of the main challenges to developing IoT applications due to the diversity of technologies and standards. IoT architecture and communication technology standardization are seen as the foundation for future IoT growth [149]. These findings suggest that one of the essential elements for the successful implementation of IoT is the use of open standards. Due to their accessibility to the general public, these standards play a significant role in fostering innovation. A collaborative consensus-based decision-making process is utilized to improve interoperability for IoT systems using various technologies [12]. Additionally, IoT architecture must provide interoperability and support full mobility to ensure uninterrupted service. Hence, using an open and standardized architecture is considered one of the main challenges in IoT [150].

Interoperability and integration of IoT face critical challenges since the development of IoT systems utilizes a range of protocols and technologies from different vendors. This leads to significant heterogeneity and interoperability problems. Therefore, it is necessary to employ a layered framework with a defined architecture to resolve this problem [151]. Considering the availability of service, coverage is a major obstacle that must be addressed in order to successfully manage the dynamics of IoT systems. Availability refers to the idea that every authorized item should have access to IoT applications at all times and from any location [152]. Ensuring smooth connectivity and desired availability requires the linked nodes to be adaptive and intelligent. Regardless of mobility, dynamic network topology change, or currently employed technologies, the network's availability and coverage area must allow for the continued use of services. All of this necessitates the use of handover, interoperability, intelligent offloading systems, and recovery procedures in the event of some unattended operations [153].

Scalability of the IoT is the ability to expand the capacity of the IoT system while maintaining the stable performance of its current services. Supporting a massive number of different devices with memory, computation, bandwidth, and other resource limitations is a major challenge in scalability [154]. Scalable procedures must be implemented for effective device detection, as well as to make those devices interoperable. A layered framework and architecture must be used to facilitate scalability and interoperability. Future IoT system development will face significant challenges in designing IoT architectures that support scalability, since they must manage a large number of system-connected devices [155].

The power and energy consumption in IoT systems is considered another challenging area, especially when it is necessary to design low-power chipsets and supply reliable power to sensors and devices [156]. This becomes more complex when the device's battery is located in distant places where it is restricted and costly to be replaced. Although the development of wireless power technologies is still in its infancy, they have the potential to send power over a considerable distance. More research should be conducted to lower device costs and power usage while increasing device capabilities (such as processing and networking), especially for edge computing nodes [157].

For edge computing nodes employed in industrial IoT (IIoT) systems, personalization and responsiveness of service problems are raised as high-priority issues [158]. Therefore, the implementation of adaptive devices to the specific needs of each connected node is essential in order to provide reliable outcomes. Moreover, taking into account the dynamic and non-deterministic nature of the industrial process, the service must be responsive, more adaptable, and realistic to future scenarios [159].

When it comes to privacy preservation, secure data transfer to the distant cloud is considered one of the most challenging issues [160]. The majority of device security and privacy concerns concern inadequate authentication and authorization, a lack of transport encryption, an insecure web interface, software, or firmware, etc. [161]. Security and privacy must be taken into account from a variety of perspectives, including legal, social, and cultural ones, to increase confidence in IoT systems. Every level of an IoT architecture needs to include security functionalities, and effective trust management must be implemented [162].

Regarding environmental issues, the environment is impacted by the Internet of Things in both beneficial and harmful ways. Since there are more and more gadgets being deployed every day, future research should pay more attention to the concept of “environmental friendliness” [12]. The sustainability of the environment is one of the biggest issues nowadays because of rising energy needs and electronic waste. To reduce the carbon footprint and, in turn, various negative effects on human health, more work should be conducted to reduce energy consumption, use renewable energy sources, and shrink the size of equipment so as to use less non-biodegradable materials. With increasing demands, the Internet uses up to 5% of global energy [163]. Therefore, this is another issue that will need to be taken into account when developing IoT-based systems in the future. New green ICT (Information and Communications Technology) enabling technologies that adhere to general green ICT principles must be considered when developing IoT systems [164].

9. IoT Future Directions

By 2030, the 6G standard for wireless communications could make it possible for IoT networks to have coverage everywhere [165]. In the 6G era, satellite-based communications are seen as an auspicious way to meet the needs of IoT services. For IoT applications, such as geo-location live tracking, eco-monitoring, and predicting of global disasters, seamless coverage everywhere and interconnection are vital. However, geostationary IoT networks like Sigfox, LoRa, and NB-IoT cannot satisfy the prerequisites of 6G IoT for broad coverage and increasing reliability [166]. On the other hand, satellite-based systems are available everywhere, can operate in any weather, and are very reliable. Therefore, satellite systems must be integrated into 6G networks to fulfil new IoT needs. Hybrid satellite–terrestrial relay network (HSTRN) technology has also been proposed to provide fully reliable communication in both high and remote areas by using terrestrial stations as relays to forward and enhance the satellite messages to the recipients [167,168].

The advance of 6G communications envisions a global, interconnected network of satellites and aerial platforms powered by AI and big data to address challenges of scalability, ultra-low-power consumption, minimal latency, privacy preservation, personalization, responsiveness, and universal coverage, even in the most inaccessible corners of the globe [169–171]. In this section, we present the most advanced research directions to address the mentioned challenges.

The need for great spectral efficiency and vast connection requires the creation of low-cost, dependable, and scalable networks [172]. The multiple access techniques used in these networks have a significant impact on their effectiveness, making it necessary to implement next-generation multiple access (NGMA) systems. Orthogonal multiple access (OMA) systems, utilized in 1G to 4G cellular networks, will no longer be able to handle the anticipated explosion in data traffic and device volume. To overcome this challenge, efficient resource allocation should be used. Effective resource distribution techniques allow for network enhancement in terms of coverage and performance. Many studies have focused on developing multiple access mechanisms to handle the exploding data traffic from IoT devices [173]. As a multiple access approach, non-orthogonal multiple access (NOMA) has attracted much interest. NOMA is superior to OMA in many respects, including its greater spectrum effectiveness, faster cell-edge performance, more relaxation at channel feedback, and lower network delay [174].

Numerous studies and deployment constraints are created by the fact that the next wave of IoT necessitates the network connectivity of a vast number of wireless devices [175]. Rate-splitting multiple access (RSMA) is regarded as a viable strategy, as it allows sequential decoding to realize the full capacity range of the multiple access network. It is a more flexible and efficient transmission mechanism than NOMA. In particular, RSMA is a helpful technique for decreasing collisions and IoT sensor networks that use random access (RA) techniques [176]. Beyond its usage in obtaining high throughput, RSMA has the potential to be used in massive IoT scenarios with a large number of connected devices [175].

Another promising technology is the re-configurable intelligent surface (RIS). For many IoT networks, RIS has become a crucial transmission mechanism [177]. RIS comprises large numbers of inexpensive passive antennas. The reflecting qualities antennas are manipulated by pin-diodes or var-actors that can intelligently organize phase shifters and tune incoming signals to target purposes [178]. The phase is adjusted to influence the radio propagation conditions by reflecting the input electromagnetic wave in a different direction. The RIS can increase the maximum user data rate. Due to these benefits, RIS has inspired much research on RIS-enhanced networks.

Facing the challenges of long-distance and universal coverage, one of the technologies that has received much interest over the last few decades is unmanned aerial vehicles (UAVs) [179]. Since UAVs are more flexible, portable, and adaptable in three-dimensional space than cellular communications, they can better establish Line-of-Sight communication and circumvent signal blocking and shadowing. From a technological standpoint, UAVs are a potentially fruitful means of achieving genuinely pervasive connections for an IoT system. On the other hand, the high cost and poor economic return of infrastructural development in isolated and inaccessible locations means terrestrial and UAV networks are unable to adequately cover the wide range of IoT devices (IoT devices) in both highly populated urban areas and uninhabited distant regions, including smart cities, smart industries, emergency tracking, and environment management [180]. To obtain universal coverage, a massive number of connections, and high-speed communications for supporting IoT devices with a broad range of services, the paradigm of a satellite and aerial-integrated network (SAIN) has the potential to employ satellite and UAV networks as an interconnected solution [173]. Furthermore, situations requiring vast coverage cannot be handled by UAVs or Low Altitude Platform Stations (LAPs) in general. Meanwhile, the High Altitude Platform Station (HAPS) has become increasingly crucial because of the broader coverage obtained by its elevated vertical position. It is distinguished from other communication structures servicing a broad region by its low price, sensitivity to delay, rapid development and deployment, and enormous capacity [181]. As a result, there is an impetus to adapt the XAPS paradigm, which uses a single HAPS as a macro aerial base station, to provide extensive coverage, and a number of LAPs, as small aerial base stations, to improve connectivity in densely populated places, outlying regions, and other challenging environments. Moreover, to improve network capacity and performance, cluster-NOMA (C-NOMA) can be integrated with the XAPS model, where terminals in HAPS are divided into multiple groups, allowing for the application of C-NOMA inside each cluster and OMA between them. Using C-NOMA with fewer terminals in each cluster might drastically decrease the decoding difficulty in comparison to NOMA [182]. This allows for more effective use of the available spectrum while also simplifying the end-user experience.

To address the low-latency challenge, fog computing's distributed and real-time solutions can be integrated into recently implemented networks [183]. Research in this area may focus on developing methods for real-time and distributed computing in fog settings, as well as exploring novel applications of fog computing [184]. Moreover, machine learning and optimization algorithms can be deployed at the edge nodes/gateways and servers to provide the required awareness of the QoS. The load on the computing servers is time-varying and nondeterministic because of the dynamic number of nodes accessing the system, especially in the case of mobile nodes. Figuring out how and when the nodes decide to offload the task by transferring the processing to the edge server presents a complicated issue [185]. When it comes to AI, edge computing is often thought of as the "final mile" because of the autonomous installation of smart services and on-edge nodes. Large numbers of edge devices (miniaturized, distributed, and reduced-power) can implement precise AI or, in coordination with other devices, for a variety of uses, such as networks of IoT nodes [48]. The intelligence for such services can be distributed to the edge to handle the task offloading challenge and satisfy the reliability and minimized-latency needs of data transfer over networks. Lyapunov optimization [186], deep reinforcement learning [187],

and graph convolution networks [188] are among the promising techniques to be integrated with edge computing in order to achieve communication-aware-computation.

The situation becomes more complex when it comes to the Space–Air–Ground IoT (SAG-IoT), in which the benefits of satellite infrastructure and aerial vehicles are integrated to enhance network coverage [189]. In this heterogeneous situation, task offloading and resource scheduling confront more difficulties due to the fact that the real SAG-IoT operates in non-deterministic spatiotemporal-dynamic scenarios [190]. Considering the long-term performance, the space–time-varying behaviors of the node task reception, transmission, and handling are random processes within a time slot rather than a snapshot of the system, due to network variation and heterogeneity characteristics. Moreover, SAG-edge and cloud servers are used up by offloading jobs; therefore, it is important to distribute them fairly because different parts of the network have varying computational needs and are subject to multiple limitations [191]. In order to reduce the total operating expenses of the network over time, real-time optimization algorithms and reinforcement learning models can be deployed to coordinate the allocation of computing resources at the local level, aerial vehicles, and edge nodes themselves [192,193]. The challenge can be addressed by employing Lyapunov optimization where the problem is broken into its subcomponents, allocating computer resources locally, reusing channels, and reusing communication channels [191,194].

10. Discussion

To realize the IoT promise of ubiquitous connectivity, the Internet has to accommodate a wide range of portable and wireless protocols for the linking of multiple devices. In this study, we took a closer look at the different integrated layers of state-of-art protocols, such as ZigBee, 6LoWPAN, BLE, LoRa, and Wi-Fi, supporting modern networks for the Internet of Things. We emphasized how challenging it is to establish a set of universal standards and an abstract framework for contrasting various IoT protocol stacks [195]. It is demanding to create a standard method to evaluate them since the documents and rules for each protocol are not always easily accessible [196]. The issue was addressed by mapping the different protocols' layers to the basic OSI stack, making it easier to identify the fundamental structure of each one. Furthermore, different parameters, including coverage, data transfer rate, RF bands, capacity, power efficiency, and the IoT environment, were used to assess and compare the performance of different technologies, as shown in Table 5. A vast volume of traffic generated by an enormous quantity of devices linked to the Internet must be managed via interoperable protocols, especially the ones exhibiting minimum consumption characteristics, such as the systems investigated in this study. The 802.15.4-based protocols, Wi-SUN, LoRa, and ZigBee, all have low power consumption characteristics. In regard to BLE, it can transmit data at a power of 1 to 10 mW [15]. The transmission power of the Wi-Fi is about 100 mW. In contrast, in terms of power utilization, IEEE 802.11ah spent higher energy for the complete transaction of a frame than IEEE 802.15.4, especially in the event of a few nodes in a low traffic scenario [197]. Nevertheless, it was shown that the power consumption of IEEE 802.11ah was comparatively greater than that of IEEE 802.15.4 in dense environments [198]. When it comes to latency-sensitive and real-time applications, current communication technologies simply cannot keep up with the ever-changing requirements imposed on infrastructure by this developing field. The infrastructure and software for the 6G Internet of Things are still in their infancy. As a result, 6G is expected to radically change the current IoT architectures and bring in a whole new era of possibilities for low-latency and high-speed applications, including upgraded service, life comfort, and user experience. Soon, the Internet of Things will be more heterogeneous, combining many complementary networks to be implemented at various times, and it will require simultaneous coping with obsolete protocols and a variety of alternative protocols.

Table 5. Summary of IoT protocols.

Characteristics	Bluetooth LE	Z-Wave	ZigBee	LoRa	6LoWPAN	Wi-Fi	PLC	
							G3	PRIME
Standard	IEEE 802.15.1	ITU G-9959	IEEE 802.15.4	IEEE 802.15.4g	IEEE 802.15.4	IEEE 802.11	ITU-T G-9903	ITU-T G-9904
Network	WPAN	WPAN	WPAN	WAN	WPAN	WLAN	WAN	
Topology	Star, mesh	Mesh	Star, mesh, tree	Mesh	Star, Mesh	Mesh		
Power	Low	Low	Low	Ultra-low-power	Low	Medium	Low	
Frequency Bands	2.4 GHz	868 MHz–908 MHz	2.4 GHz	869/915 MHz	868 MHz (EU), 915 MHz (USA), 2.4 GHz (Global)	2.4/5/6 GHz	3–490 kHz	3–95 kHz
Data Rate	1–2 Mbps	40 kbps	250 kbps	50 kbps	250 kbps	11–9600 Mbps	33.4 kbps	130 kbps
Range	15–30 m Short Range	30 m (indoors), 100 m (outdoors)	10–100 m Short Range	Urban (2–5 km) suburban (15 km)	10–100 m Short Range	100m	10 m–100 Kms	
Spreading	FHSS	-	DSSS	CSS	DSSS	DSSS		
Security	E0 stream, AES-128	AES-128	AES-128	AES-128	AES-128	WPA2/3		
Common Applications	Audio applications and Wireless headsets	Home Monitoring and Control	Controlling and Home industry monitoring	Air Pollution Monitoring. Agriculture Processing. Animal Tracking. Fire Detection. Fleet Tracking. Home Security.	Monitor and Control via internet	Mobile, Business, Home, Computerized, Automotive, Browsing	Smart Grid	

11. Conclusions

The concept of the IoT has quickly spread throughout modern society with the purpose of improving the quality of life by integrating intelligent devices, applications, and technologies that automate everything around us. This paper discussed the most important elements of the IoT paradigm, as well as its protocols, technologies, and applications. The discussion provided examples of the various operational and efficiency properties of every protocol. Thereby, this should serve as a solid groundwork for scholars and practitioners keen on learning more about the IoT techniques and protocols to comprehend the IoT's general structure and the function of the various parts and protocols, which makes it easier to select the suitable protocol and its simulation tool for any application. In conclusion, we believe that the next IoT generation will be universal in its coverage, intelligent in its offloading and resource allocation decisions, aware of the QoS, and more secure against cyber-attacks, facilitating efficient communication between the physical and cloud levels.

Author Contributions: Conceptualization, A.S. and L.A.S.; methodology, M.M., A.G. and A.S.; formal analysis, L.A.S., N.H. and A.S.; investigation, L.A.S., N.H. and A.S.; resources, M.M., A.G. and A.S., writing—original draft preparation, M.M., A.G. and A.I.A.; writing—review and editing, L.A.S., N.H., A.S. and A.E.; visualization, M.M. and A.G.; supervision, A.S., N.H. and L.A.S.; project administration, A.S. and L.A.S. funding acquisition, A.S. and N.H. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by Information Technology Academia Collaboration (ITAC) grant number CFP207.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: There are no available data to be stated.

Acknowledgments: Authors would like to thank El Sewedy Electrometer Group (EMG) company for supporting the research done in this work.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

3G	Third Generation
3GPP	Third Generation Partnership Project
4G	Fourth Generation
5G	Fifth Generation
6G	Sixth Generation
6LoWPAN	IPv6 over Low-power Wireless Personal Area Networks
A/V	Audio/Video
AC	Alternative Current
AES	Advanced Encryption Standard
AI	Artificial Intelligence
AMI	Advanced Metering Infrastructure
AMP	Alternative
AMQP	Advanced Message Queuing Protocol
AP	Access Point
APF	Application Framework
APS	Application Sublayer
BLE	Bluetooth Low Energy
BR	Bluetooth Basic Rate
BPSK	Binary Phase-Shift Keying
CA	Collision Avoidance
CoAP	Constrained Application Protocol
CPU	Central Processing Unit
CSMA	Carrier Sense Multiple Access
DC	Direct Current
DODAG	Destination Oriented Directed Acyclic Graph
DPSK	Differential Phase Shift Keying
FAN	Field Area Network
EDR	Enhanced Data Rate
FPGAs	Field Programmable Gate Arrays
FSK	Frequency Shift Keying
GFSK	Gaussian Frequency Shift Keying
GPS	Global Positioning System
HARQ	Hybrid Automatic Repeat Request
HAN	Home Area Network
HS	High Speed
HSTRN	Hybrid Satellite–Terrestrial Relay Network
HTTP	Hypertext Transfer Protocol
I/O	Input/Output
IDC	International Data Corporation
IEEE	Institute of Electrical and Electronics Engineers
IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force
IIoT	Industrial Internet of Things
IoT	Internet of Things
IoTds	IoT devices
IPv6	Internet Protocol version 6
IT	Information Technology
ISM	Industrial, Scientific, and Medical
ISO	International Organization for Standardization
JUTA	Japan Utility Telemetry Association
LAN	Local Area Network
LAPS	Low Altitude Platform Station
LE	Low energy
LEDL	Light Emitting Diode
LL-AC	Low-Latency Access Category
LOADng	On-demand Ad hoc Distance-vector Routing Protocol–Next Generation

LoRa	Long Range
LoRaWAN	Long Range Wide Area Network
LPWAN	Low-Power Wide Area Network
LTE	Long-Term Evolution
HAPS	High Altitude Platform Station
MAC	Media Access layer
ML	Machine Learning
M2M	Machine-to-machine
MQTT	Message Queue Telemetry Transpor
MU-MIMO	Multi-User, Multiple-Input, Multiple-Output technology
NB-IoT	NarrowBand-Internet of Things
NB-PLC	Narrowband PLC
NFC	Near Field Communication
NGMA	Next-Generation Multiple Access
NOMA	Non-Orthogonal Multiple Access
OFDMA	Orthogonal Frequency Division Multiple Access
OMA	Orthogonal multiple access
OSI	Open Systems Interconnection
PAN	Personal Area Network
PHY	Physical layer
PAM	Pulse Amplitude Modulation
PLC	Power Line Communication
PRIME	Powerline Intelligent Metering Evolution
QoS	Quality of Service
QR	Quick Response
QAM	Quadrature Amplitude Modulation
RA	Random Access
RF	Radio frequency
RFID	Radio Frequency Identification
RIS	Re-configurable Intelligent Surface
RLMM	Resource-Limited Monitoring and Management
RPL	Routing Protocol
RSMA	Rate-Splitting Multiple Access
SAIN	Satellite and Aerial-Integrated Network
SIG	Special Interest Group
SiP	systems-in-package
SoC	Systems-on-Chip
SSL	Secure Sockets Layer
UAVs	Unmanned Aerial Vehicles
SUN	Smart Utility Network
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TSN	Time-Sensitive Networking
TX	Transmission
TXOP	Transmission Opportunity
WAN	Wide Area Network
WGs	Working Groups
Wi-Fi	Wireless Fidelity
Wi-SUN	Wireless Smart Utility Network
WLANs	Wireless LANs
WSN	Wireless Sensor Network
VR	Virtual Reality
XML	eXtensible Markup Language
XMPP	Extensible Messaging and Presence Protocol
ZCL	Zigbee Cluster Library
ZDO	Zigbee Device Object

References

1. Khorov, E.; Lyakhov, A.; Krotov, A.; Guschin, A. A survey on IEEE 802.11ah: An enabling networking technology for smart cities. *Comput. Commun.* **2015**, *58*, 53–69. [\[CrossRef\]](#)
2. Darabkh, K.A.; Alfawares, M.G.; Althunibat, S. MDRMA: Multi-data rate mobility-aware AODV-based protocol for flying ad-hoc networks. *Veh. Commun.* **2019**, *18*, 100163. [\[CrossRef\]](#)
3. Michalski, A.; Watral, Z. Problems of Powering End Devices in Wireless Networks of the Internet of Things. *Energies* **2021**, *14*, 2417. [\[CrossRef\]](#)
4. Alhasanat, M.; Althunibat, S.; Darabkh, K.A.; Alhasanat, A.; Alsafasfeh, M. A physical-layer key distribution mechanism for IoT networks. *Mob. Netw. Appl.* **2020**, *25*, 173–178. [\[CrossRef\]](#)
5. Hendriks, S. Internet of Things: How the World Will Be Connected in 2025. Master's Thesis, Utrecht University, Utrecht, The Netherlands, 2016.
6. Milić, D.C.; Tolić, I.H.; Peko, M. Internet of Things (IoT) solutions in smart transportation management. In Proceedings of the Business Logistics in Modern Management, Osijek, Croatia, 5–6 October 2020.
7. Wytrebowicz, J.; Cabaj, K.; Krawiec, J. Messaging Protocols for IoT Systems—A Pragmatic Comparison. *Sensors* **2021**, *21*, 6904. [\[CrossRef\]](#)
8. Sadeghi-Niaraki, A. Internet of Thing (IoT) review of review: Bibliometric overview since its foundation. *Future Gener. Comput. Syst.* **2023**, *143*, 361–377. [\[CrossRef\]](#)
9. Miorandi, D.; Sicari, S.; De Pellegrini, F.; Chlamtac, I. Internet of things: Vision, applications and research challenges. *Ad Hoc Networks* **2012**, *10*, 1497–1516. [\[CrossRef\]](#)
10. Said, O.; Masud, M. Towards internet of things: Survey and future vision. *Int. J. Comput. Networks* **2013**, *5*, 1–17.
11. Guth, J.; Breitenbücher, U.; Falkenthal, M.; Fremantle, P.; Kopp, O.; Leymann, F.; Reinfurt, L. A Detailed Analysis of IoT Platform Architectures: Concepts, Similarities, and Differences. In *Internet of Everything: Algorithms, Methodologies, Technologies and Perspectives*; Di Martino, B., Li, K.C., Yang, L.T., Esposito, A., Eds.; Springer Singapore: Singapore, 2018; pp. 81–101. [\[CrossRef\]](#)
12. Čolaković, A.; Hadžialić, M. Internet of Things (IoT): A review of enabling technologies, challenges, and open research issues. *Comput. Networks* **2018**, *144*, 17–39. [\[CrossRef\]](#)
13. Gerodimos, A.; Maglaras, L.; Ferrag, M.A.; Ayres, N.; Kantzavelou, I. IoT: Communication protocols and security threats. *Internet Things Cyber-Phys. Syst.* **2023**, *3*, 1–13. [\[CrossRef\]](#)
14. Domínguez-Bolaño, T.; Campos, O.; Barral, V.; Escudero, C.J.; García-Naya, J.A. An overview of IoT architectures, technologies, and existing open-source projects. *Internet Things* **2022**, *20*, 100626. [\[CrossRef\]](#)
15. Elkhodr, M.; Shahrestani, S.; Cheung, H. Emerging Wireless Technologies in the Internet of Things: A Comparative Study. *Int. J. Wirel. Mob. Networks* **2016**, *8*, 67–82. [\[CrossRef\]](#)
16. Al-Sarawi, S.; Anbar, M.; Alieyan, K.; Alzubaidi, M. Internet of Things (IoT) communication protocols. In Proceedings of the 2017 8th International Conference on Information Technology (ICIT), Amman, Jordan, 17–18 May 2017; pp. 685–690.
17. Burhan, M.; Rehman, R.A.; Khan, B.; Kim, B.S. IoT Elements, Layered Architectures and Security Issues: A Comprehensive Survey. *Sensors* **2018**, *18*, 2796. [\[CrossRef\]](#)
18. Salman, T.; Jain, R. A Survey of Protocols and Standards for Internet of Things. *arXiv* **2017**, arXiv:1903.11549.
19. Bayılmış, C.; Ebleme, M.A.; Çavuşoğlu, Ü.; Küçük, K.; Sevin, A. A survey on communication protocols and performance evaluations for Internet of Things. *Digit. Commun. Networks* **2022**, *8*, 1094–1104. [\[CrossRef\]](#)
20. Florea, I.; Rughinis, R.; Ruse, L.; Dragomir, D. Survey of Standardized Protocols for the Internet of Things. In Proceedings of the 2017 21st International Conference on Control Systems and Computer Science (CSCS), Bucharest, Romania, 19–31 May 2017; pp. 190–196. [\[CrossRef\]](#)
21. Mehta, R.; Sahni, J.; Khanna, K. Internet of things: Vision, applications and challenges. *Procedia Comput. Sci.* **2018**, *132*, 1263–1269. [\[CrossRef\]](#)
22. Bonetto, R.; Bui, N.; Lakkundi, V.; Olivereau, A.; Serbanati, A.; Rossi, M. Secure communication for smart IoT objects: Protocol stacks, use cases and practical examples. In Proceedings of the 2012 IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM), San Francisco, CA, USA, 25–28 June 2012; pp. 1–7.
23. Ray, P.P. A survey on Internet of Things architectures. *J. King Saud Univ.-Comput. Inf. Sci.* **2018**, *30*, 291–319. [\[CrossRef\]](#)
24. Rose, K.; Eldridge, S.; Chapin, L. The internet of things: An overview. *Internet Soc.* **2015**, *80*, 1–50.
25. Goulart, A.; Chennamaneni, A.; Torre, D.; Hur, B.; Al-Aboosi, F.Y. On Wide-Area IoT Networks, Lightweight Security and Their Applications—A Practical Review. *Electronics* **2022**, *11*, 1762. [\[CrossRef\]](#)
26. Lin, J.; Yu, W.; Zhang, N.; Yang, X.; Zhang, H.; Zhao, W. A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications. *IEEE Internet Things J.* **2017**, *4*, 1125–1142. [\[CrossRef\]](#)
27. Qiu, T.; Chen, N.; Li, K.; Atiquzzaman, M.; Zhao, W. How Can Heterogeneous Internet of Things Build Our Future: A Survey. *IEEE Commun. Surv. Tutor.* **2018**, *20*, 2011–2027. [\[CrossRef\]](#)
28. Mashal, I.; Alsaryrah, O.; Chung, T.Y.; Yang, C.Z.; Kuo, W.H.; Agrawal, D.P. Choices for interaction with things on Internet and underlying issues. *Ad Hoc Netw.* **2015**, *28*, 68–90. [\[CrossRef\]](#)
29. Abdmeziem, M.R.; Tandjaoui, D.; Romdhani, I. Architecting the internet of things: State of the art. In *Robots and Sensor Clouds*; Springer: Berlin/Heidelberg, Germany, 2016; pp. 55–75.

30. Verma, D.; Singh, K.R.; Yadav, A.K.; Nayak, V.; Singh, J.; Solanki, P.R.; Singh, R.P. Internet of things (IoT) in nano-integrated wearable biosensor devices for healthcare applications. *Biosens. Bioelectron. X* **2022**, *11*, 100153. [[CrossRef](#)]
31. Oliveira, L.; Rodrigues, J.J.; Kozlov, S.A.; Rabêlo, R.A.; de Albuquerque, V.H.C. MAC layer protocols for internet of things: A survey. *Future Internet* **2019**, *11*, 16. [[CrossRef](#)]
32. Farooq, M.U.; Waseem, M.; Mazhar, S.; Khairi, A.; Kamal, T. A review on internet of things (IoT). *Int. J. Comput. Appl.* **2015**, *113*, 1–7.
33. Vashi, S.; Ram, J.; Modi, J.; Verma, S.; Prakash, C. Internet of Things (IoT): A vision, architectural elements, and security issues. In Proceedings of the 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Palladam, India, 10–11 February 2017; pp. 492–496. [[CrossRef](#)]
34. Gupta, S.; Gupta, A.; Shankar, G. Cloud Computing: Services, Deployment Models and Security Challenges. In Proceedings of the 2021 2nd International Conference on Smart Electronics and Communication (ICOSEC), Trichy, India, 7–9 October 2021; pp. 414–418. [[CrossRef](#)]
35. Alotaibi, A.; Barnawi, A. Securing massive IoT in 6G: Recent solutions, architectures, future directions. *Internet Things* **2023**, *22*, 100715. [[CrossRef](#)]
36. Sethi, P.; Sarangi, S.R. Internet of Things: Architectures, Protocols, and Applications. *J. Electr. Comput. Eng.* **2017**, *2017*, 9324035. [[CrossRef](#)]
37. Munir, A.; Kansakar, P.; Khan, S.U. IFCIoT: Integrated Fog Cloud IoT: A novel architectural paradigm for the future Internet of Things. *IEEE Consum. Electron. Mag.* **2017**, *6*, 74–82. [[CrossRef](#)]
38. Singh, R.; Kovacs, J.; Kiss, T. To offload or not? an analysis of big data offloading strategies from edge to cloud. In Proceedings of the 2022 IEEE World AI IoT Congress (AIoT), Seattle, WA, USA, 6–9 June 2022; pp. 46–52.
39. Wang, X.; Han, Y.; Leung, V.C.M.; Niyato, D.; Yan, X.; Chen, X. Convergence of Edge Computing and Deep Learning: A Comprehensive Survey. *IEEE Commun. Surv. Tutorials* **2020**, *22*, 869–904. [[CrossRef](#)]
40. Pujol, V.C.; Dustdar, S. Fog robotics—Understanding the research challenges. *IEEE Internet Comput.* **2021**, *25*, 10–17. [[CrossRef](#)]
41. Kumar, P.; Gupta, G.P.; Tripathi, R. A distributed ensemble design based intrusion detection system using fog computing to protect the internet of things networks. *J. Ambient. Intell. Humaniz. Comput.* **2021**, *12*, 9555–9572. [[CrossRef](#)]
42. Abouaomar, A.; Cherkaoui, S.; Mlika, Z.; Kobbane, A. Resource Provisioning in Edge Computing for Latency-Sensitive Applications. *IEEE Internet Things J.* **2021**, *8*, 11088–11099. [[CrossRef](#)]
43. Laroui, M.; Nour, B.; Mounghla, H.; Cherif, M.A.; Afifi, H.; Guizani, M. Edge and fog computing for IoT: A survey on current research activities & future directions. *Comput. Commun.* **2021**, *180*, 210–231. [[CrossRef](#)]
44. Iftikhar, S.; Gill, S.S.; Song, C.; Xu, M.; Aslanpour, M.S.; Toosi, A.N.; Du, J.; Wu, H.; Ghosh, S.; Chowdhury, D.; et al. AI-based fog and edge computing: A systematic review, taxonomy and future directions. *Internet Things* **2023**, *21*, 100674. [[CrossRef](#)]
45. Shakarami, A.; Shakarami, H.; Ghobaei-Arani, M.; Nikougoftar, E.; Faraji-Mehmandar, M. Resource provisioning in edge/fog computing: A Comprehensive and Systematic Review. *J. Syst. Archit.* **2022**, *122*, 102362. [[CrossRef](#)]
46. Zhang, T.; Shen, Z.; Jin, J.; Zheng, X.; Tagami, A.; Cao, X. Achieving Democracy in Edge Intelligence: A Fog-Based Collaborative Learning Scheme. *IEEE Internet Things J.* **2021**, *8*, 2751–2761. [[CrossRef](#)]
47. McEnroe, P.; Wang, S.; Liyanage, M. A survey on the convergence of edge computing and AI for UAVs: Opportunities and challenges. *IEEE Internet Things J.* **2022**, *9*, 15435–15459. [[CrossRef](#)]
48. Zhang, Y.; Yu, H.; Zhou, W.; Man, M. Application and Research of IoT Architecture for End-Net-Cloud Edge Computing. *Electronics* **2023**, *12*, 1. [[CrossRef](#)]
49. Singh, R.; Gill, S.S. Edge AI: A survey. *Internet Things-Cyber-Phys. Syst.* **2023**, *3*, 71–92. [[CrossRef](#)]
50. Manowska, A.; Wycisk, A.; Nowrot, A.; Pielot, J. The Use of the MQTT Protocol in Measurement, Monitoring and Control Systems as Part of the Implementation of Energy Management Systems. *Electronics* **2023**, *12*, 17. [[CrossRef](#)]
51. Yassein, M.B.; Shatnawi, M.Q.; Aljwarneh, S.; Al-Hatmi, R. Internet of Things: Survey and open issues of MQTT protocol. In Proceedings of the 2017 International Conference on engineering & MIS (ICEMIS), Monastir, Tunisia, 8–10 May 2017; pp. 1–6.
52. Arvind, S.; Narayanan, V.A. An overview of security in CoAP: Attack and analysis. In Proceedings of the 2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS), Coimbatore, India, 15–16 March 2019; pp. 655–660.
53. Naik, N. Choice of effective messaging protocols for IoT systems: MQTT, CoAP, AMQP and HTTP. In Proceedings of the 2017 IEEE International Systems Engineering Symposium (ISSE), Vienna, Austria, 11–13 October 2017; pp. 1–7.
54. Yokotani, T.; Sasaki, Y. Comparison with HTTP and MQTT on required network resources for IoT. In Proceedings of the 2016 International Conference on Control, Electronics, Renewable Energy and Communications (ICCEREC), Bandung, Indonesia, 13–15 September 2016; pp. 1–6.
55. Nikolov, N. Research of MQTT, CoAP, HTTP and XMPP IoT Communication protocols for Embedded Systems. In Proceedings of the 2020 XXIX International Scientific Conference Electronics (ET), Sozopol, Bulgaria, 16–18 September 2020; pp. 1–4. [[CrossRef](#)]
56. Sun, L.; Chen, Y.; Cheng, Q.; Zhu, B.; Chen, C.; Hou, X. Communication Application of Distributed Energy Resources Monitoring System Based on XMPP. In Proceedings of the 2021 International Conference on Computer Engineering and Artificial Intelligence (ICCEAI), Shanghai, China, 21–29 August 2021; pp. 66–70. [[CrossRef](#)]
57. Hofer-Schmitz, K.; Stojanović, B. Towards formal verification of IoT protocols: A Review. *Comput. Networks* **2020**, *174*, 107233. [[CrossRef](#)]

58. Deniz, E.; Samet, R. A New Model for Secure Joining to ZigBee 3.0 Networks in the Internet of Things. In Proceedings of the 2018 International Congress on Big Data, Deep Learning and Fighting Cyber Terrorism (IBIGDELFT), Ankara, Turkey, 3–4 December 2018; pp. 102–106. [CrossRef]
59. Adi, P.D.P.; Sihombing, V.; Siregar, V.M.M.; Yanris, G.J.; Sianturi, F.A.; Purba, W.; Tamba, S.P.; Simatupang, J.; Arifuddin, R.; Subairi, et al. A Performance Evaluation of ZigBee Mesh Communication on the Internet of Things (IoT). In Proceedings of the 2021 3rd East Indonesia Conference on Computer and Information Technology (EIConCIT), Surabaya, Indonesia, 9–11 April 2021; pp. 7–13. [CrossRef]
60. Gavra, V.D.; Pop, O.A. Usage of ZigBee and LoRa wireless technologies in IoT systems. In Proceedings of the 2020 IEEE 26th International Symposium for Design and Technology in Electronic Packaging (SIITME), Pitesti, Romania, 21–24 October 2020; pp. 221–224. [CrossRef]
61. Cheruvu, S.; Kumar, A.; Smith, N.; Wheeler, D.M. *Demystifying Internet of Things SECURITY: Successful Iot Device/Edge and Platform Security Deployment*; Springer: Berlin/Heidelberg, Germany, 2020.
62. Zeadally, S.; Siddiqui, F.; Baig, Z. 25 Years of Bluetooth Technology. *Future Internet* **2019**, *11*, 194. [CrossRef]
63. Fatihah, S.N.; Dewa, G.R.R.; Park, C.; Sohn, I. Self-Optimizing Bluetooth Low Energy Networks for Industrial IoT Applications. *IEEE Commun. Lett.* **2023**, *27*, 386–390. [CrossRef]
64. Ortiz, J.C.G.; Silvestre-Blanes, J.; Sempere-Payá, V.M.; Frau, D.C. Evaluation of improvements in BLE Mesh through CODED PHY. In Proceedings of the 2021 26th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA), Vasteras, Sweden, 7–10 September 2021; pp. 1–4. [CrossRef]
65. Pallavi, S.; Narayanan, V.A. An Overview of Practical Attacks on BLE Based IOT Devices and Their Security. In Proceedings of the 2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS), Coimbatore, India, 15–16 March 2019; pp. 694–698. [CrossRef]
66. Chadha, S.S.; Singh, M.; Pardeshi, S.K. Bluetooth technology: Principle, applications and current status. *Int. J. Comput. Sci. Commun.* **2013**, *4*, 16–30.
67. Cao, S.; Chen, X.; Yuan, B. Overview of Short-range Wireless Communication Protocol. In Proceedings of the 2022 7th International Conference on Computer and Communication Systems (ICCCS), Wuhan, China, 22–25 April 2022; pp. 519–523.
68. Kalanandhini, G.; Aravind, A.; Vijayalakshmi, G.; Gayathri, J.; Senthilkumar, K. Bluetooth technology on IoT using the architecture of Piconet and Scatternet. *AIP Conf. Proc.* **2022**, *2393*, 020121.
69. Woolley, M. The Bluetooth Low Energy Primer. *Bluetooth Blog* **2022**, *15*, 2022. Available online: <https://www.bluetooth.com/blog/introducing-the-bluetooth-low-energy-primer/> (accessed on 11 April 2023).
70. Badihi, B.; Ghavimi, F.; Jäntti, R. On the system-level performance evaluation of Bluetooth 5 in IoT: Open office case study. In Proceedings of the 2019 16th International Symposium on Wireless Communication Systems (ISWCS), Oulu, Finland, 22–29 September 2019; pp. 485–489.
71. Spörk, M.; Boano, C.A.; Römer, K. Performance and trade-offs of the new PHY modes of BLE 5. In Proceedings of the ACM MobiHoc Workshop on Pervasive Systems in the IoT Era, Catania, Italy, 2 July 2019; pp. 7–12.
72. Raza, S.; Misra, P.; He, Z.; Voigt, T. Building the Internet of Things with bluetooth smart. *Ad Hoc Networks* **2017**, *57*, 19–31. [CrossRef]
73. Darroudi, S.M.; Gomez, C. Bluetooth Low Energy Mesh Networks: A Survey. *Sensors* **2017**, *17*, 1467. [CrossRef]
74. Alfiah, F.; Ningtyas, S.; Sudaryanti, T.; Astuti, R.; Gumelar, R.T. Increase Comfort and Security in a Smart Home Using a Prediction Algorithm and Z-Wave Protocol. *Int. J. Eng. Tech.* **2018**, *4*, 179–185.
75. Yassein, M.B.; Mardini, W.; Khalil, A. Smart homes automation using Z-wave protocol. In Proceedings of the 2016 International Conference on Engineering & MIS (ICEMIS), Agadir, Morocco, 22–24 September 2016; pp. 1–6. [CrossRef]
76. Linh An, P.m.; Kim, T. A Study of the Z-Wave Protocol: Implementing Your Own Smart Home Gateway. In Proceedings of the 2018 3rd International Conference on Computer and Communication Systems (ICCCS), Nagoya, Japan, 27–30 April 2018; pp. 411–415. [CrossRef]
77. Danbatta, S.J.; Varol, A. Comparison of Zigbee, Z-Wave, Wi-Fi, and Bluetooth Wireless Technologies Used in Home Automation. In Proceedings of the 2019 7th International Symposium on Digital Forensics and Security (ISDFS), Barcelos, Portugal, 10–12 June 2019; pp. 1–5. [CrossRef]
78. Algani, Y.M.; Balaji, S.; AlbertRaj, A.; Elangovan, G.; Sathish Kumar, P.J.; Agordzo, G.K.; Pentang, J.T.; Kiran Bala, B. Integration of Internet Protocol and Embedded System On IoT Device Automation. 2021. Available online: <https://www.researchsquare.com/article/rs-947704/v1> (accessed on 11 April 2023).
79. Pimple, N.; Salunke, T.; Pawar, U.; Sangoi, J. Wireless Security—An Approach Towards Secured Wi-Fi Connectivity. In Proceedings of the 2020 6th International Conference on Advanced Computing and Communication Systems (ICACCS), Coimbatore, India, 6–7 March 2020; pp. 872–876. [CrossRef]
80. Fan, S.; Ge, Y.; Yu, X. Comparison Analysis and Prediction of Modern Wi-Fi Standards. In Proceedings of the 2022 International Conference on Big Data, Information and Computer Network (BDICN), Sanya, China, 20–22 January 2022; pp. 581–585. [CrossRef]
81. Tian, L.; Santi, S.; Seferagić, A.; Lan, J.; Famaey, J. Wi-Fi HaLow for the Internet of Things: An up-to-date survey on IEEE 802.11ah research. *J. Netw. Comput. Appl.* **2021**, *182*, 103036. [CrossRef]
82. Chakravarthi, V.S. M2M Communication in Constrained Devices. In *Internet of Things and M2M Communication Technologies: Architecture and Practical Design Approach to IoT in Industry 4.0*; Springer: Cham, Switzerland, 2021; pp. 191–206.

83. Zhang, L.; Ma, M. FKR: An efficient authentication scheme for IEEE 802.11ah networks. *Comput. Secur.* **2020**, *88*, 101633. [[CrossRef](#)]
84. Rochim, A.F.; Harijadi, B.; Purbanugraha, Y.P.; Fuad, S.; Nugroho, K.A. Performance comparison of wireless protocol IEEE 802.11ax vs. 802.11ac. In Proceedings of the 2020 International Conference on Smart Technology and Applications (ICoSTA), Surabaya, Indonesia, 20 February 2020; pp. 1–5. [[CrossRef](#)]
85. Yang, M.; Li, B.; Yan, Z. MAC Technology of IEEE 802.11ax: Progress and Tutorial. *Mob. Networks Appl.* **2020**, *26*, 1122–1136. [[CrossRef](#)]
86. Avallone, S.; Imputato, P.; Redieteb, G.; Ghosh, C.; Roy, S. Will OFDMA Improve the Performance of 802.11 Wifi Networks? *IEEE Wirel. Commun.* **2021**, *28*, 100–107. [[CrossRef](#)]
87. Bankov, D.; Khorov, E.; Lyakhov, A.; Sandal, M. Enabling real-time applications in Wi-Fi networks. *Int. J. Distrib. Sens. Networks* **2019**, *15*, 1550147719845312. [[CrossRef](#)]
88. Gokhale, V.; Eid, M.; Kroep, K.; Prasad, R.V.; Rao, V.S. Toward Enabling High-Five Over WiFi: A Tactile Internet Paradigm. *IEEE Commun. Mag.* **2021**, *59*, 90–96. [[CrossRef](#)]
89. 802.11ax-2021-IEEE Standard for Information Technology—Telecommunications and Information Exchange between Systems Local and Metropolitan Area Networks—Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 1: Enhancements for High-Efficiency WLAN; IEEE: Washington, DC, USA, 2021; pp. 1–767. [[CrossRef](#)]
90. Shukla, S.; Hassan, M.F.; Khan, M.K.; Jung, L.T.; Awang, A. An analytical model to minimize the latency in healthcare internet-of-things in fog computing environment. *PLoS ONE* **2019**, *14*, e4934. [[CrossRef](#)]
91. Qadri, Y.A.; Zulqarnain.; Nauman, A.; Musaddiq, A.; Garcia-Villegas, E.; Kim, S.W. Preparing Wi-Fi 7 for Healthcare Internet-of-Things. *Sensors* **2022**, *22*, 6209. [[CrossRef](#)]
92. Deng, C.; Fang, X.; Han, X.; Wang, X.; Yan, L.; He, R.; Long, Y.; Guo, Y. IEEE 802.11be Wi-Fi 7: New Challenges and Opportunities. *IEEE Commun. Surv. Tutorials* **2020**, *22*, 2136–2166. [[CrossRef](#)]
93. Yang, Z.; Chang, C.H. 6LoWPAN Overview and Implementations. In Proceedings of the EWSN, Beijing, China, 25–27 February 2019; pp. 357–361.
94. Kasinathan, P.; Pastrone, C.; Spirito, M.A.; Vinkovits, M. Denial-of-Service detection in 6LoWPAN based Internet of Things. In Proceedings of the 2013 IEEE 9th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), Lyon, France, 7–9 October 2013; pp. 600–607.
95. Alkama, L.; Bouallouche-Medjkoune, L. IEEE 802.15.4 historical revolution versions: A survey. *Computing* **2021**, *103*, 99–131. [[CrossRef](#)]
96. Musaddiq, A.; Zikria, Y.B.; Zulqarnain; Kim, S.W. Routing protocol for Low-Power and Lossy Networks for heterogeneous traffic network. *EURASIP J. Wirel. Commun. Netw.* **2020**, *2020*, 21. [[CrossRef](#)]
97. Ioulianou, P.P.; Vassilakis, V.G. Denial-of-service attacks and countermeasures in the RPL-based Internet of Things. In *Computer Security*; Springer: Berlin/Heidelberg, Germany, 2019; pp. 374–390.
98. Zhao, L.; Wang, G. Research Status of 6LoWPAN in the Field of Internet of Things. In Proceedings of the 2020 5th International Conference on Automation, Control and Robotics Engineering (CACRE), Dalian, China, 19–20 September 2020; pp. 739–743. [[CrossRef](#)]
99. Okumura, R.; Mizutani, K.; Harada, H. A broadcast protocol for IEEE 802.15. 4e RIT based Wi-SUN systems. In Proceedings of the 2017 IEEE 85th Vehicular Technology Conference (VTC Spring), Sydney, Australia, 4–8 June 2017; pp. 1–5.
100. Anani, W.; Ouda, A.; Hamou, A. A Survey Of Wireless Communications for IoT Echo-Systems. In Proceedings of the 2019 IEEE Canadian Conference of Electrical and Computer Engineering (CCECE), Edmonton, AB, Canada, 5–8 May 2019; pp. 1–6. [[CrossRef](#)]
101. Harada, H.; Mizutani, K.; Fujiwara, J.; Mochizuki, K.; Obata, K.; Okumura, R. IEEE 802.15. 4g based Wi-SUN communication systems. *IEICE Trans. Commun.* **2017**, *100*, 1032–1043. [[CrossRef](#)]
102. Hirakawa, R.; Okumura, R.; Mizutani, K.; Harada, H. A Novel Routing Method with Load-Balancing in Wi-SUN FAN Network. In Proceedings of the 2021 IEEE 7th World Forum on Internet of Things (WF-IoT), New Orleans, LA, USA, 14–31 June 2021; pp. 362–367. [[CrossRef](#)]
103. Kashiwagi, Y.; Harada, H.; Masaki, H.; Osumi, K. Development of Evaluation Systems for Large-Scale Wi-SUN FAN-Based IoT Applications. In Proceedings of the 2022 IEEE 33rd Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC), Virtual, 15–20 September 2022; pp. 1–6. [[CrossRef](#)]
104. Raychowdhury, A.; Pramanik, A. Survey on LoRa technology: Solution for internet of things. In *Intelligent Systems, Technologies and Applications*; Springer: Berlin/Heidelberg, Germany, 2020; pp. 259–271.
105. Sinha, R.S.; Wei, Y.H. A survey on LPWA technology: LoRa and NB-IoT. *ICT Express* **2017**, *3*, 14–21. [[CrossRef](#)]
106. Şenyuva, R.V. Comparison of LoRa-Based Modulations. In Proceedings of the 2022 30th Signal Processing and Communications Applications Conference (SIU), Safranbolu, Turkey, 16–18 May 2022; pp. 1–4. [[CrossRef](#)]
107. Zhang, C.; Yue, J.; Jiao, L.; Shi, J.; Wang, S. A Novel Physical Layer Encryption Algorithm for LoRa. *IEEE Commun. Lett.* **2021**, *25*, 2512–2516. [[CrossRef](#)]
108. Rama, Y.; Özpınar, M.A. A comparison of long-range licensed and unlicensed LPWAN technologies according to their geolocation services and commercial opportunities. In Proceedings of the 2018 18th Mediterranean Microwave Symposium (MMS), Istanbul, Turkey, 31 October–2 November 2018; pp. 398–403.

109. Nikoukar, A.; Raza, S.; Poole, A.; Güneş, M.; Dezfouli, B. Low-power wireless for the internet of things: Standards and applications. *IEEE Access* **2018**, *6*, 67893–67926. [[CrossRef](#)]
110. Locatelli, P.; Spadaccino, P.; Cuomo, F. Ruling Out IoT Devices in LoRaWAN. In Proceedings of the IEEE INFOCOM 2022—IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Virtual, 2–5 May 2022; pp. 1–2. [[CrossRef](#)]
111. Dangana, M.; Ansari, S.; Abbasi, Q.H.; Hussain, S.; Imran, M.A. Suitability of NB-IoT for indoor industrial environment: A survey and insights. *Sensors* **2021**, *21*, 5284. [[CrossRef](#)] [[PubMed](#)]
112. Medina-Acosta, G.; Zhang, L.; Chen, J.; Uesaka, K.; Wang, Y.; Lundqvist, O.; Bergman, J. 3GPP Release-17 Physical Layer Enhancements for LTE-M and NB-IoT. *IEEE Commun. Stand. Mag.* **2022**, *6*, 80–86. [[CrossRef](#)]
113. Ugwuanyi, S.; Paul, G.; Irvine, J. Survey of IoT for developing countries: Performance analysis of LoRaWAN and cellular nb-IoT networks. *Electronics* **2021**, *10*, 2224. [[CrossRef](#)]
114. Sanchez-Gomez, J.; Carrillo, D.G.; Sanchez-Iborra, R.; Hernández-Ramos, J.L.; Granjal, J.; Marin-Perez, R.; Zamora-Izquierdo, M.A. Integrating LPWAN Technologies in the 5G Ecosystem: A Survey on Security Challenges and Solutions. *IEEE Access* **2020**, *8*, 216437–216460. [[CrossRef](#)]
115. Wang, Y.P.E.; Lin, X.; Adhikary, A.; Grovlen, A.; Sui, Y.; Blankenship, Y.; Bergman, J.; Razaghi, H.S. A primer on 3GPP narrowband Internet of Things. *IEEE Commun. Mag.* **2017**, *55*, 117–123. [[CrossRef](#)]
116. Ali, M.S.; Li, Y.; Jewel, M.K.H.; Famoriji, O.J.; Lin, F. Channel Estimation and Peak-to-Average Power Ratio Analysis of Narrowband Internet of Things Uplink Systems. *Wirel. Commun. Mob. Comput.* **2018**, *2018*, 1–15. [[CrossRef](#)]
117. Mahbub, M. NB-IoT: Applications and future prospects in perspective of Bangladesh. *Int. J. Inf. Technol.* **2020**, *12*, 1183–1193. [[CrossRef](#)]
118. Abrahamsen, F.E.; Ai, Y.; Cheffena, M. Communication technologies for smart grid: A comprehensive survey. *Sensors* **2021**, *21*, 8087. [[CrossRef](#)]
119. Tonello, A.M.; De Pianta, M. Exploring Joint Voltage and Impedance Modulation in Wired Networks. In Proceedings of the 2020 IEEE International Symposium on Power Line Communications and its Applications (ISPLC), Malaga, Spain, 11–13 May 2020; pp. 1–6.
120. Ndolo, A.; Çavdar, İ.H. Current state of communication systems based on electrical power transmission lines. *J. Electr. Syst. Inf. Technol.* **2021**, *8*, 1–10. [[CrossRef](#)]
121. Noura, H.N.; Melki, R.; Chehab, A.; Fernandez, J.H. Efficient and robust data availability solution for hybrid PLC/RF systems. *Comput. Netw.* **2021**, *185*, 107675. [[CrossRef](#)]
122. Zhilenkov, A.A.; Gilyazov, D.D.; Matveev, I.I.; Krishtal, Y.V. Power line communication in IoT-systems. In Proceedings of the 2017 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus), Moscow, Russia, 1–3 June 2017; pp. 242–245. [[CrossRef](#)]
123. Saleem, M.S. Development of PLC based communication architecture for battery management system. In Proceedings of the 2020 IEEE 91st Vehicular Technology Conference (VTC2020-Spring), Antwerp, Belgium, 25–28 May 2020; pp. 1–5.
124. Fazio, A.; Erseghe, T.; Ghiani, E.; Murrioni, M.; Siano, P.; Silvestro, F. Integration of renewable energy sources, energy storage systems, and electrical vehicles with smart power distribution networks. *J. Ambient. Intell. Humaniz. Comput.* **2013**, *4*, 663–671. [[CrossRef](#)]
125. Masood, B.; Baig, S. Channel modeling of NB-PLC for Smart Grid. In Proceedings of the 2015 IEEE Symposium on Computers and Communication (ISCC), Washington, DC, USA, 6–9 July 2015; pp. 745–750.
126. Sadowski, Z. Comparison of PLC-PRIME and PLC-G3 protocols. In Proceedings of the 2015 International School on Nonsinusoidal Currents and Compensation (ISNCC), Lagow, Poland, 25–28 June 2015; pp. 1–6.
127. Razazian, K.; Umari, M.; Kamalizad, A.; Loginov, V.; Navid, M. G3-PLC specification for powerline communication: Overview, system simulation and field trial results. In Proceedings of the ISPLC2010, Rio de Janeiro, Brazil, 28–31 March 2010; pp. 313–318.
128. Kenny, J.P.; Wilke, J.J.; Ulmer, C.D.; Baker, G.M.; Knight, S.; Friesen, J.A. An Evaluation of Ethernet Performance for Scientific Workloads. In Proceedings of the 2020 IEEE/ACM Innovating the Network for Data-Intensive Science (INDIS), Atlanta, GA, USA, 12 November 2020; pp. 57–67. [[CrossRef](#)]
129. Conti, M.; Donadel, D.; Turrin, F. A survey on industrial control system testbeds and datasets for security research. *IEEE Commun. Surv. Tutorials* **2021**, *23*, 2248–2294. [[CrossRef](#)]
130. Min, J.; Park, Y. Performance Enhancement of In-Vehicle 10BASE-T1S Ethernet Using Node Prioritization and Packet Segmentation. *IEEE Access* **2022**, *10*, 103286–103295. [[CrossRef](#)]
131. Sanz, A.; Ibar, J.C.; Lacasa, L. PLC-RF hybrid communication systems, model and simulation. In Proceedings of the 2021 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm), Aachen, Germany, 25–28 October 2021; pp. 158–163.
132. Lavenu, C.; Chauvenet, C.; Treffiletti, P.; Varesio, M.; Hueske, K. Standardization Challenges, Opportunities and Recent Evolutions for the G3-PLC Technology. *Energies* **2021**, *14*, 1937. [[CrossRef](#)]
133. Zhang, Y.; Mao, J. An Overview of the Development of Antenna-in-Package Technology for Highly Integrated Wireless Devices. *Proc. IEEE* **2019**, *107*, 2265–2280. [[CrossRef](#)]
134. Zandberg, K.; Schleiser, K.; Acosta, F.; Tschofenig, H.; Baccelli, E. Secure Firmware Updates for Constrained IoT Devices Using Open Standards: A Reality Check. *IEEE Access* **2019**, *7*, 71907–71920. [[CrossRef](#)]

135. Bansal, S.; Kumar, D. IoT ecosystem: A survey on devices, gateways, operating systems, middleware and communication. *Int. J. Wirel. Inf. Netw.* **2020**, *27*, 340–364. [[CrossRef](#)]
136. Baccelli, E.; Gündoğan, C.; Hahm, O.; Kietzmann, P.; Lenders, M.S.; Petersen, H.; Schleiser, K.; Schmidt, T.C.; Wählich, M. RIOT: An open source operating system for low-end embedded devices in the IoT. *IEEE Internet Things J.* **2018**, *5*, 4428–4440. [[CrossRef](#)]
137. Živković, M.; Nikolić, B.; Protić, J.; Popović, R. A survey and classification of wireless sensor networks simulators based on the domain of use. *Adhoc Sens. Wirel. Netw.* **2014**, *20*, 245–287.
138. Troiano, G.O.; Ferreira, H.S.; Trindade, F.C.; Ochoa, L.F. Co-simulator of power and communication networks using OpenDSS and OMNeT++. In Proceedings of the 2016 IEEE Innovative Smart Grid Technologies-Asia (ISGT-Asia) IEEE, Melbourne, Australia, 28 November–1 December 2016; pp. 1094–1099.
139. Kumar, S.; Bansal, A. Performance investigation of topology-based routing protocols in flying ad-hoc networks using NS-2. In *IoT and Cloud Computing Advancements in Vehicular Ad-Hoc Networks*; IGI Global: Hershey, PA, USA, 2020; pp. 243–267.
140. Kim, B.S.; Sung, T.E.; Kim, K.I. An ns-3 implementation and experimental performance analysis of IEEE 802.15.6 standard under different deployment scenarios. *Int. J. Environ. Res. Public Health* **2020**, *17*, 4007. [[CrossRef](#)]
141. Keramidas, G.; Voros, N.; Hübner, M. *Components and Services for IoT Platforms*; Springer: Berlin/Heidelberg, Germany, 2016.
142. Bautista, P.A.B.; Urquiza-Aguiar, L.F.; Cárdenas, L.L.; Igartua, M.A. Large-scale simulations manager tool for OMNeT++: Expediting simulations and post-processing analysis. *IEEE Access* **2020**, *8*, 159291–159306. [[CrossRef](#)]
143. Le, T.D.; Anwar, A.; Beuran, R.; Loke, S.W. Smart grid co-simulation tools: Review and cybersecurity case study. In Proceedings of the 2019 7th International Conference on Smart Grid (icSmartGrid) IEEE, Newcastle, Australia, 9–11 December 2019; pp. 39–45.
144. Nasiakou, A.; Alamaniotis, M.; Tsoukalas, L.H. MatGridGUI—A toolbox for GridLAB-D simulation platform. In Proceedings of the 2016 7th International Conference on Information, Intelligence, Systems & Applications (IISA) IEEE, Patras, Greece, 11–16 June 2016; pp. 1–5.
145. Chaturvedi, D.K. *Modeling and Simulation of Systems Using MATLAB® and Simulink®*; CRC Press: Boca Raton, FL, USA, 2017.
146. Klee, H.; Allen, R. *Simulation of Dynamic Systems with MATLAB® and Simulink®*; CRC Press: Boca Raton, FL, USA, 2018.
147. Patel, R.L.; Pathak, M.J.; Nayak, A.J. Survey on network simulators. *Int. J. Comput. Appl.* **2018**, *182*, 23–30. [[CrossRef](#)]
148. Lohiya, R.; Thakkar, A. Application Domains, Evaluation Data Sets, and Research Challenges of IoT: A Systematic Review. *IEEE Internet Things J.* **2021**, *8*, 8774–8798. [[CrossRef](#)]
149. Shah, S.W.H.; Mian, A.N.; Aijaz, A.; Qadir, J.; Crowcroft, J. Energy-Efficient MAC for Cellular IoT: State-of-the-Art, Challenges, and Standardization. *IEEE Trans. Green Commun. Netw.* **2021**, *5*, 587–599. [[CrossRef](#)]
150. Rana, M.M.; Dahotre, N. IoT-Based Cyber-Physical Additive Manufacturing Systems: A Secure Communication Architecture, Research Challenges and Directions. In Proceedings of the 2021 6th International Conference on Inventive Computation Technologies (ICICT), Coimbatore, India, 20–22 January 2021; pp. 216–219. [[CrossRef](#)]
151. Dave, M.; Doshi, J.; Arolkar, H. MQTT-CoAP Interconnector: IoT Interoperability Solution for Application Layer Protocols. In Proceedings of the 2020 Fourth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Palladam, India, 7–9 October 2020; pp. 122–127. [[CrossRef](#)]
152. Ishaq, M.; Afzal, M.H.; Tahir, S.; Ullah, K. A Compact Study of Recent Trends of Challenges and Opportunities in Integrating Internet of Things (IoT) and Cloud Computing. In Proceedings of the 2021 International Conference on Computing, Electronic and Electrical Engineering (ICE Cube), Quetta, Pakistan, 11–12 April 2021; pp. 1–4. [[CrossRef](#)]
153. Mustafa, J.; Sandström, K.; Ericsson, N.; Rizvanovic, L. Analyzing availability and QoS of service-oriented cloud for industrial IoT applications. In Proceedings of the 2019 24th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA), Zaragoza, Spain, 10–13 September 2019; pp. 1403–1406. [[CrossRef](#)]
154. Djonov, M.; Galabov, M.; Georgieva-Trifonova, T. Solving IoT Security and Scalability Challenges with Blockchain. In Proceedings of the 2021 5th International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT), Ankara, Turkey, 21–23 October 2021; pp. 52–56. [[CrossRef](#)]
155. Razzaq, A. Microservices Architecture for IoT Applications in the Ocean: Microservices Architecture based Framework for Reducing the Complexity and Increasing the Scalability of IoT Applications in the Ocean. In Proceedings of the 2020 20th International Conference on Computational Science and Its Applications (ICCSA), Cagliari, Italy, 1–4 July 2020; pp. 87–90. [[CrossRef](#)]
156. Bansal, S.; Tomar, V. Challenges & Security Threats in IoT with Solution Architectures. In Proceedings of the 2022 2nd International Conference on Power Electronics & IoT Applications in Renewable Energy and its Control (PARC), Mathura, India, 21–22 January 2022; pp. 1–5. [[CrossRef](#)]
157. Yassein, M.B.; Hmeidi, I.; Meqdadi, O.; Alghazo, F.; Odat, B.; AlZoubi, O.; Smairat, A. Challenges and Techniques of Constrained Application Protocol (CoAP) for Efficient Energy Consumption. In Proceedings of the 2020 11th International Conference on Information and Communication Systems (ICICS), Irbid, Jordan, 7–9 April 2020; pp. 373–377. [[CrossRef](#)]
158. Foukalas, F.; Tziouvaras, A. Edge Artificial Intelligence for Industrial Internet of Things Applications: An Industrial Edge Intelligence Solution. *IEEE Ind. Electron. Mag.* **2021**, *15*, 28–36. [[CrossRef](#)]
159. Sun, W.; Liu, J.; Yue, Y. AI-Enhanced Offloading in Edge Computing: When Machine Learning Meets Industrial IoT. *IEEE Network* **2019**, *33*, 68–74. [[CrossRef](#)]
160. Georgiana Dorobantu, O.; Halunga, S. Security threats in IoT. In Proceedings of the 2020 International Symposium on Electronics and Telecommunications (ISETC), Timisoara, Romania, 5–6 November 2020; pp. 1–4. [[CrossRef](#)]

161. Bonkra, A.; Dhiman, P. IoT Security Challenges in Cloud Environment. In Proceedings of the 2021 2nd International Conference on Computational Methods in Science & Technology (ICCMST), Mohali, India, 17–18 December 2021; pp. 30–34. [\[CrossRef\]](#)
162. Abdul Sattar, K.; Al-Omary, A. A survey: Security issues in IoT environment and IoT architecture. In Proceedings of the 3rd Smart Cities Symposium (SCS 2020), Virtual, 21–23 September 2020; Volume 2020, pp. 96–102. [\[CrossRef\]](#)
163. Gubbi, J.; Buyya, R.; Marusic, S.; Palaniswami, M. Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Gener. Comput. Syst.* **2013**, *29*, 1645–1660.
164. Landum, M.; Moura, M.; Reis, L. ICT Good Practices in alignment with Green IT. In Proceedings of the 2020 15th Iberian Conference on Information Systems and Technologies (CISTI), Sevilla, Spain, 17–20 June 2020; pp. 1–6. [\[CrossRef\]](#)
165. Zong, B.; Fan, C.; Wang, X.; Duan, X.; Wang, B.; Wang, J. 6G Technologies: Key Drivers, Core Requirements, System Architectures, and Enabling Technologies. *IEEE Veh. Technol. Mag.* **2019**, *14*, 18–27. [\[CrossRef\]](#)
166. Ye, N.; Yu, J.; Wang, A.; Zhang, R. Help from space: Grant-free massive access for satellite-based IoT in the 6G era. *Digit. Commun. Networks* **2022**, *8*, 215–224. [\[CrossRef\]](#)
167. Bankey, V.; Upadhyay, P.K. Physical Layer Security of Multiuser Multirelay Hybrid Satellite-Terrestrial Relay Networks. *IEEE Trans. Veh. Technol.* **2019**, *68*, 2488–2501. [\[CrossRef\]](#)
168. Niu, H.; Lin, Z.; Chu, Z.; Zhu, Z.; Xiao, P.; Nguyen, H.X.; Lee, I.; Al-Dhahir, N. Joint Beamforming Design for Secure RIS-Assisted IoT Networks. *IEEE Internet Things J.* **2023**, *10*, 1628–1641. [\[CrossRef\]](#)
169. Giordani, M.; Polese, M.; Mezzavilla, M.; Rangan, S.; Zorzi, M. Toward 6G Networks: Use Cases and Technologies. *IEEE Commun. Mag.* **2020**, *58*, 55–61. [\[CrossRef\]](#)
170. Qadir, Z.; Le, K.N.; Saeed, N.; Munawar, H.S. Towards 6G Internet of Things: Recent advances, use cases, and open challenges. *ICT Express* **2022**. [\[CrossRef\]](#)
171. Kök, İ.; Okay, F.Y.; Özdemir, S. FogAI: An AI-supported fog controller for Next Generation IoT. *Internet Things* **2022**, *19*, 100572. [\[CrossRef\]](#)
172. Tegos, S.A.; Diamantoulakis, P.D.; Lioumpas, A.S.; Sarigiannidis, P.G.; Karagiannidis, G.K. Slotted ALOHA with NOMA for the next generation IoT. *IEEE Trans. Commun.* **2020**, *68*, 6289–6301. [\[CrossRef\]](#)
173. Lin, Z.; Lin, M.; de Cola, T.; Wang, J.B.; Zhu, W.P.; Cheng, J. Supporting IoT With Rate-Splitting Multiple Access in Satellite and Aerial-Integrated Networks. *IEEE Internet Things J.* **2021**, *8*, 11123–11134. [\[CrossRef\]](#)
174. Lin, Z.; Lin, M.; Wang, J.B.; de Cola, T.; Wang, J. Joint Beamforming and Power Allocation for Satellite-Terrestrial Integrated Networks With Non-Orthogonal Multiple Access. *IEEE J. Sel. Top. Signal Process.* **2019**, *13*, 657–670. [\[CrossRef\]](#)
175. Kumar, A.; Li, F.Y.; Martinez-Bauset, J. Revealing the Benefits of Rate-Splitting Multiple Access for Uplink IoT Traffic. In Proceedings of the GLOBECOM 2022—2022 IEEE Global Communications Conference, Rio de Janeiro, Brazil, 4–8 December 2022; pp. 111–116. [\[CrossRef\]](#)
176. Liu, H.; Tsiftsis, T.A.; Kim, K.J.; Kwak, K.S.; Poor, H.V. Rate splitting for uplink NOMA with enhanced fairness and outage performance. *IEEE Trans. Wirel. Commun.* **2020**, *19*, 4657–4670. [\[CrossRef\]](#)
177. Agrawal, N.; Bansal, A.; Singh, K.; Li, C.P.; Mumtaz, S. Finite Block Length Analysis of RIS-Assisted UAV-Based Multiuser IoT Communication System With Non-Linear EH. *IEEE Trans. Commun.* **2022**, *70*, 3542–3557. [\[CrossRef\]](#)
178. Bansal, A.; Singh, K.; Li, C.P. Analysis of hierarchical rate splitting for intelligent reflecting surfaces-aided downlink multiuser MISO communications. *IEEE Open J. Commun. Soc.* **2021**, *2*, 785–798. [\[CrossRef\]](#)
179. Li, B.; Fei, Z.; Zhang, Y. UAV Communications for 5G and Beyond: Recent Advances and Future Trends. *IEEE Internet Things J.* **2019**, *6*, 2241–2263. [\[CrossRef\]](#)
180. Ruan, Y.; Li, Y.; Zhang, R.; Cheng, W.; Liu, C. Cooperative Resource Management for Cognitive Satellite-Aerial-Terrestrial Integrated Networks Towards IoT. *IEEE Access* **2020**, *8*, 35759–35769. [\[CrossRef\]](#)
181. Zhou, D.; Gao, S.; Liu, R.; Gao, F.; Guizani, M. Overview of development and regulatory aspects of high altitude platform system. *Intell. Conver. Networks* **2020**, *1*, 58–78. [\[CrossRef\]](#)
182. Qin, P.; Zhu, Y.; Zhao, X.; Feng, X.; Liu, J.; Zhou, Z. Joint 3D-Location Planning and Resource Allocation for XAPS-Enabled C-NOMA in 6G Heterogeneous Internet of Things. *IEEE Trans. Veh. Technol.* **2021**, *70*, 10594–10609. [\[CrossRef\]](#)
183. Zare, M.; Elmi Sola, Y.; Hasanpour, H. Towards distributed and autonomous IoT service placement in fog computing using asynchronous advantage actor-critic algorithm. *J. King Saud Univ. Comput. Inf. Sci.* **2023**, *35*, 368–381. [\[CrossRef\]](#)
184. Gomes, E.; Costa, F.; De Rolt, C.; Plentz, P.; Dantas, M. A Survey from Real-Time to Near Real-Time Applications in Fog Computing Environments. *Telecom* **2021**, *2*, 489–517. [\[CrossRef\]](#)
185. Alghamdi, I.; Anagnostopoulos, C.; Pezaros, D.P. Data quality-aware task offloading in Mobile Edge Computing: An Optimal Stopping Theory approach. *Future Gener. Comput. Syst.* **2021**, *117*, 462–479. [\[CrossRef\]](#)
186. Li, Y.; Wang, X.; Gan, X.; Jin, H.; Fu, L.; Wang, X. Learning-aided computation offloading for trusted collaborative mobile edge computing. *IEEE Trans. Mob. Comput.* **2019**, *19*, 2833–2849. [\[CrossRef\]](#)
187. Baek, J.; Kaddoum, G. Online partial offloading and task scheduling in SDN-Fog networks with deep recurrent reinforcement learning. *IEEE Internet Things J.* **2021**, *9*, 11578–11589. [\[CrossRef\]](#)
188. Chen, J.; Yang, Y.; Wang, C.; Zhang, H.; Qiu, C.; Wang, X. Multitask offloading strategy optimization based on directed acyclic graphs for edge computing. *IEEE Internet Things J.* **2021**, *9*, 9367–9378. [\[CrossRef\]](#)
189. Zhang, Z.; Xiao, Y.; Ma, Z.; Xiao, M.; Ding, Z.; Lei, X.; Karagiannidis, G.K.; Fan, P. 6G Wireless Networks: Vision, Requirements, Architecture, and Key Technologies. *IEEE Veh. Technol. Mag.* **2019**, *14*, 28–41. [\[CrossRef\]](#)

190. Zhou, C.; Wu, W.; He, H.; Yang, P.; Lyu, F.; Cheng, N.; Shen, X. Deep Reinforcement Learning for Delay-Oriented IoT Task Scheduling in SAGIN. *IEEE Trans. Wirel. Commun.* **2021**, *20*, 911–925. [[CrossRef](#)]
191. Qin, P.; Fu, Y.; Zhao, X.; Wu, K.; Liu, J.; Wang, M. Optimal Task Offloading and Resource Allocation for C-NOMA Heterogeneous Air-Ground Integrated Power Internet of Things Networks. *IEEE Trans. Wirel. Commun.* **2022**, *21*, 9276–9292. [[CrossRef](#)]
192. Tang, F.; Hofner, H.; Kato, N.; Kaneko, K.; Yamashita, Y.; Hangai, M. A Deep Reinforcement Learning-Based Dynamic Traffic Offloading in Space-Air-Ground Integrated Networks (SAGIN). *IEEE J. Sel. Areas Commun.* **2022**, *40*, 276–289. [[CrossRef](#)]
193. Al Ridhawi, I.; Otoum, S. Supporting Next-Generation Network Management with Intelligent Moving Devices. *IEEE Network* **2022**, *36*, 8–15. [[CrossRef](#)]
194. Liu, J.; Zhao, X.; Qin, P.; Geng, S.; Meng, S. Joint Dynamic Task Offloading and Resource Scheduling for WPT Enabled Space-Air-Ground Power Internet of Things. *IEEE Trans. Netw. Sci. Eng.* **2022**, *9*, 660–677. [[CrossRef](#)]
195. Al-Fuqaha, A.; Guizani, M.; Mohammadi, M.; Aledhari, M.; Ayyash, M. Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. *IEEE Commun. Surv. Tutorials* **2015**, *17*, 2347–2376. [[CrossRef](#)]
196. Tournier, J.; Lesueur, F.; Mouël, F.L.; Guyon, L.; Ben-Hassine, H. A survey of IoT protocols and their security issues through the lens of a generic IoT stack. *Internet Things* **2021**, *16*, 100264. [[CrossRef](#)]
197. Mahbub, M. Progressive researches on IoT security: An exhaustive analysis from the perspective of protocols, vulnerabilities, and preemptive architectonics. *J. Netw. Comput. Appl.* **2020**, *168*, 102761. [[CrossRef](#)]
198. Kassab, W.; Darabkh, K.A. A–Z survey of Internet of Things: Architectures, protocols, applications, recent advances, future directions and recommendations. *J. Netw. Comput. Appl.* **2020**, *163*, 102663. [[CrossRef](#)]

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.