Hindawi
Wireless Communications and Mobile Computing
Volume 2018, Article ID 5349894, 24 pages
https://doi.org/10.1155/2018/5349894

Review Article

Network Protocols, Schemes, and Mechanisms for Internet of Things (IoT): Features, Open Challenges, and Trends

Anna Triantafyllou,[1] **Panagiotis Sarigiannidis**,[1] **and Thomas D. Lagkas**[2]

[1]*Department of Informatics and Telecommunications Engineering, University of Western Macedonia, Kozani 50100, Greece*
[2]*Computer Science Department, The University of Sheffield International Faculty, CITY College, Thessaloniki 54626, Greece*

Correspondence should be addressed to Thomas D. Lagkas; t.lagkas@sheffield.ac.uk

Received 29 March 2018; Revised 30 July 2018; Accepted 9 August 2018; Published 13 September 2018

Academic Editor: Juan F. Valenzuela-Valdés

Internet of Things (IoT) constitutes the next step in the field of technology, bringing enormous changes in industry, medicine, environmental care, and urban development. Various challenges are to be met in forming this vision, such as technology interoperability issues, security and data confidentiality requirements, and, last but not least, the development of energy efficient management systems. In this paper, we explore existing networking communication technologies for the IoT, with emphasis on encapsulation and routing protocols. The relation between the IoT network protocols and the emerging IoT applications is also examined. A thorough layer-based protocol taxonomy is provided, while how the network protocols fit and operate for addressing the recent IoT requirements and applications is also illustrated. What is the most special feature of this paper, compared to other survey and tutorial works, is the thorough presentation of the inner schemes and mechanisms of the network protocols subject to IPv6. Compatibility, interoperability, and configuration issues of the existing and the emerging protocols and schemes are discussed based on the recent advanced of IPv6. Moreover, open networking challenges such as security, scalability, mobility, and energy management are presented in relation to their corresponding features. Lastly, the trends of the networking mechanisms in the IoT domain are discussed in detail, highlighting future challenges.

1. Introduction

In recent years, the use of the Internet has become a necessity in many aspects of the everyday life. The vision of a global networking platform based on the smart objects communication has already made a big leap forward. The so-called Internet of Things (IoT) technology grows into a need for modern society, where people and things are virtually integrated, forming thus information systems, through wireless sensor nodes and networks [1]. This innovation will pave the way to the development of new applications and services, which will be able to leverage the connectivity of physical and virtual entities [2].

The IoT paradigm relies on existing communication technologies such as Bluetooth, ZigBee, WiFi, and Long Term Evolution-Advanced (LTE-A), just to name a few. However, forming an acceptable and desirable IoT system, based on these various technologies, seems a laborious challenge. The standardization of IoT is crucial in providing advanced interoperability for all sensor devices and objects, which also require an identity management system. Furthermore, network security as well as data confidentiality raises major issues [3]. Last but not least, efficient energy and data management systems are required, with the aim of greening the IoT systems [4]. All of these challenges need to be addressed according to the adopted type of networking technologies. Although several studies have been conducted concerning the IoT communication technologies [5–10], none of them deals with the IoT network layer, also known as transmission layer, and its technologies. More specifically, in [5], current and emerging technologies for supporting wide area Machine-to-Machine (M2M) networks based on IoT devices were presented, while [6] was focused on the standards for IoT in the fields of data communications, services, and support for (M2M)/IoT applications. The authors in [7] presented an overview of the enabling applications, protocols,

technologies, and the recent research endeavors which address various aspects of IoT. In [8], a brief overview of the IETF protocol suite was proposed to support IoT devices and applications. Similarly, in [11], different standards offered by the Internet Engineering Task Force (IETF), the Institute of Electrical and Electronics Engineers (IEEE), and the International Telecommunication Union (ITU) for the IoT were discussed. Furthermore, [9] was focused on the evolution of Wireless Sensor Networks (WSNs), as a critical part of the IoT architecture, while sketching a framework able to harmonize new IoT installations and non-IP implementation. A similar study was conducted in [10], where recent work on low energy consuming networking for WSN systems and IoT was presented.

This paper deals with the task of presenting the IoT network layer and its challenges as a separate field of research that keeps being partially and inadequately analysed through other works that concern specific use cases of the IoT technology or standardization efforts in different architectural layers. The contribution of this work is a complete analysis and taxonomy of all suitable network communication technologies for the IoT platform regardless of the network topology, communication range, or intended application usage. In literature, the term 'IoT technology' tends to become confusing since it can be used for specifying protocols from every architectural layer of the IoT platform. Aiming to provide a better understanding of the IoT architecture and technologies usage, the presented taxonomy contributes to efficiently separating suitable IoT technologies into data link layer protocols, network encapsulation protocols, and routing protocols according to each standard. Towards this direction, another taxonomy concerning the IoT middleware contributes to presenting the basic components and architectural types of this basic IoT layer. The IoT middleware provides efficient service management towards the development of applications, based on the information provided by the network layer in the IoT infrastructure. Due to this fact, providing knowledge on the implementation and technologies of these two layers is quite beneficial. Compared to [12], our work goes beyond presenting the basic communication technologies and their challenges and limitations, by compiling, discussing, and presenting in detail the role, the functionality, the advantages, and disadvantages of most important standards, protocols, and schemes of the IoT network layer. As a result, a comprehensive discussion of each technology is enclosed, while the present challenges and drawbacks of each technology are highlighted. In addition, emphasis is given on the ability of each standard to adopt the IPv6 protocol, which offers many benefits to IoT development and infrastructure. Furthermore, possible solutions and remedies are suggested for addressing current gaps and deficiencies of each technology, leading to efficient network communication between the IoT objects in line with the latest trends in the IoT domain. The conducted survey can also provide motivation to scholars and professionals towards developing new and more efficient networking protocols, based on the current gaps and deficiencies discussed.

The rest of the paper is organized as follows. In Section 2, the IoT vision, components, architecture, and applications are introduced. In Section 3, the most important existing technologies, protocols, and schemes are presented, followed by a detailed taxonomy according to the IoT architecture and networking challenges. Section 4 refers to the comparison of the IoT network protocols by dividing them into two separate categories, the encapsulation and routing protocols, since these together form the network layer. Open networking challenges are mentioned and discussed in Section 5, while Section 6 is devoted to discussing current trends of the IoT domain. Finally, Section 7 concludes this survey.

2. The Internet of Things

2.1. IoT Vision and Smart Objects. IoT is the evolution of Internet posing immense challenges in data collection, analysis, and distribution towards a more productive use of information in order to improve the quality of life [13]. The concept of IoT involves the management of sensors or devices distributed around the network, so as to recognize and notify users instantly about real-time events [14]. These devices, having basic computational skills, are called smart objects. Smart objects are characterized by a unique identifier, i.e., a name tag for device description and an address for communication. According to [15] there are three types of smart objects:

(i) Activity: aware objects that can collect data regarding work activities as well as their own use

(ii) Policy: aware objects that can translate activities and events with respect to specified organizational policies

(iii) Process: aware objects, where a process is a set of relevant tasks and activities which are ordered based on their position in space and time

IoT devices are mainly characterized by their constrained resources in terms of power, processing, memory, and bandwidth. Due to this fact, traditional protocols concerning network operations and security cannot be implemented in IoT specific environment, with their current form [16–18]. However, it is the fact that, by providing embedded security to the devices by design, a lot of benefits are offered, concerning cost reduction in security architecture, increasing reliability, and improving general performance [17].

2.2. IoT Applications. Due to the use of smart objects, IoT is considered to have a huge impact on a wide variety of applications, such as WSNs and narrowband communications [19]. Figure 1 outlines the most important IoT applications. IoT can find its application in almost every aspect of our everyday life. One of the most compelling applications of IoT exist in conceptualizing smart cities, smart homes, and smart object security. Typical examples of practical IoT services in smart environments are (a) traffic monitoring, (b) measuring environmental parameters, and (c) performing surveillance of spaces and equipment maintenance. For instance, medical applications aim to improve life quality by monitoring the patient's activities. Moreover, IoT is beneficial in monitoring processes in industry and preventing the occurrence of

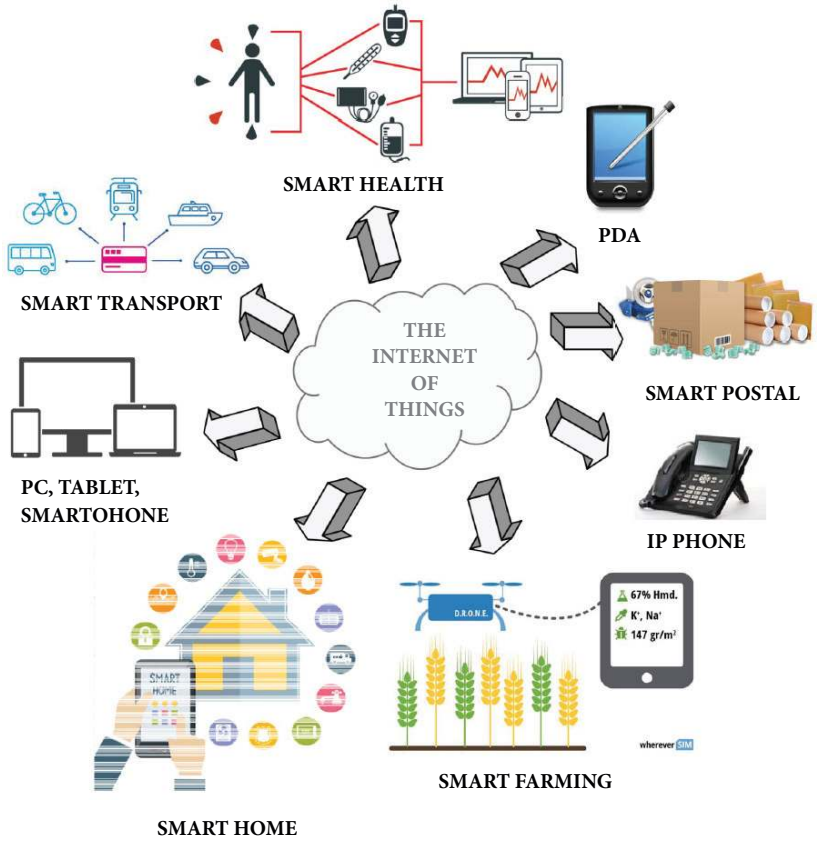

Figure 1: IoT applications.

dangerous implications caused by environmental damage. Intelligent farming systems are also an important IoT application, aiming at increasing the agricultural productivity by avoiding conditions which are considered inappropriate for farming [4]. However, intelligent systems require a well-structured network and a smart management system. As a result, a lot of studies have been focused on the architecture of the IoT platform [20].

Table 1 presents the most important IoT application domains and their related applications. The design of smart cities and smart homes seems to be the flagship of IoT applications. IoT technologies allow the system development of advanced traffic control, monitoring the air quality and efficiently lighting up of the city. Smart city lighting is evolving rapidly because of the confluence of multiple technological revolutions. Smart lighting is evolving to visually interconnect cities together with the use of interactive sensors and digital displays [21]. In addition, smart parking devices systems are emerged for allowing fast end easy tracking of available parking spaces. Furthermore, sensors usage is further expanded for detecting traffic violations and forwarding the relevant information to law enforcement services [2].

Intelligent transportation systems are also an attractive IoT application. IoT can provide a set of smart tools for facilitating the implementation of a connected, integrated, and automated transportation system which could be information-intensive. To this end, a more efficient provisioning of the user interests is feasible, while such a system could be further enhanced for being responsive to the needs of travelers and system operators [22].

Systems of home automation are undoubtedly attractive, because they enable controlling everything through Web applications in a remote manner [23]. In a smart home, energy consumption management will be possible. Also, emergencies could be timely detected, while interaction with appliances can be achieved and a more advanced home security system could be feasible. Smart grid is another compelling topic of the IoT domain, where an intelligent system of electrical distribution that bidirectionally delivers flows of energy from producers to consumers [24] could be provided. Contrary to the legacy power grids, where only a few power plants centrally generate the energy which is 'broadcasted' to the end users via a large network of substations, transformers, and cables, in the smart grid the final customers can be also producers [23]. In particular, the smart grid makes use of IoT technologies for leveraging fault detection and allowing self-healing of the network without the intervention of technicians. As a result, more reliable supply of electricity is supported and the risk of natural disasters and cyber-attacks is minimized.

IoT technology is suitable for environmental monitoring applications by measuring natural parameters (such as temperature, humidity, rainfall, wind, and river height). On this ground, IoT technologies can facilitate the creation of

Table 1: Domains and related applications of IoT.

APPLICATION DOMAIN	APPLICATION
Smart mobility & smart tourism	Traffic management, multi-modal transport Road condition monitoring, parking system, waste collection Payment systems, tour guide services
Public safety & environmental monitoring	Environmental & territorial monitoring Video/radar/satellite surveillance Emergency site/rescue personal tracking, emergency plan
Smart Home	Plant maintenance, energy management Video surveillance, access management, children protection Entertainment, comfortable living
Smart Grid	Load management, storage service, entertainment services Sustainable mobility, booking charging slot Power generation/distribution/storage, energy management
Industrial processing	Real-time vehicle diagnostic, assistance driving Luggage management, boarding operation, mobile tickets Monitoring industrial plants
Agriculture & breeding	Animal tracking, certification and trade control Irrigation, monitoring agricultural production & feed Farm registration management
Logistics & product lifetime management	Identification of materials/product deterioration Waterhouse management, retail, inventory Shopping operation, fast payment
Medical & healthcare	Remote monitoring medical parameters, diagnostics Medical equipment tracking, secure indoor envir. management Smart hospital services, entertainment services
Independent living	Elderly assistance, disabled assistance Personal home/mobile assistance, social inclusion Individual well-being, personal behavior impact on society

new decision support and monitoring systems, providing advanced granularity and real-time features over existing approaches [4].

An additional important application is the development of a smart fire detection system. To this end, fire departments timely receive information which in turn is used for making efficient decisions and supporting actions, for instance, the description of the area affected by the fire and the possible presence of inflammable materials and people. Furthermore, IoT applications in the fields of surveillance and security are substantial. Surveillance of spaces has become necessary for enterprise buildings such as factory floors, shopping malls, car parks, and a variety of other public places [23].

IoT technologies may be also adopted in the industry for real-time monitoring of product availability and maintaining proper stock inventory [2]. In this way the occurrence of dangerous implications, caused by environmental damage, can be prevented. However, industrial IoT is not limited to manufacturing and factory applications. The maturity of the technology and its cyber-physical control capabilities has spread its use outside traditional factory environments. IoT applications now constitute a significant part of the critical infrastructure at many fronts.

Moreover, the design of intelligent transportation systems will enhance transportation management and control employing advanced technology of information collection, sensing devices, and networking [4].

One other important field involves medical applications, where a better quality of patient life is ensured through medical-based IoT services. Sensors, either fixed (proximity) or wearable (e.g., gyroscopes and accelerometers), will be employed to collect information used to monitor the activities of patients within their living environments [2]. For instance, in [25], a medical system was developed that measures and detects human-heartbeat and body temperature of the patient. Moreover, a system for navigating blind and visually impaired people indoors was presented in [7] by using IoT-based components.

Benefits will be also present with the creation of an intelligent farming system, aiming to enhance agricultural efficiency by identifying optimal farming conditions [4]. As presented in [26], the concept of the Agricultural IoT (AIoT) utilizes networking technology in agricultural production. The hardware part of this agricultural IoT platform includes temperature monitoring, humidity measuring, and light sensors and processors with large data processing capabilities. These hardware devices are connected by short-range wireless networking technologies, such as Bluetooth, ZigBee, and WiFi.

2.3. IoT Middleware. The IoT provides numerous opportunities and facilitates the implementation of all the above application scenarios. However, the effective management of smart objects within the infrastructure remains challenging so as

to achieve efficient communication between physical components while maintaining quality of service in the cyber world. The desired interoperability factor in order to hide the details of different technologies is fundamental to allow IoT developers not to be concerned with software services that are not directly relevant to the specific IoT application. This ability is offered by the middleware. The use of middleware is considered in being an ideal fit with IoT application development, since it simplifies the establishment of new applications and services in complex IoT distributed infrastructures with numerous heterogeneous devices [27]. IoT middleware allows developers and users to experiment IoT devices. Based on an architectural point of view, a service-based IoT middleware can be focused on providing the deployment of devices as services [28]. On the other hand, a cloud-based IoT middleware enables users to interpret easily the data they have collected. However, the type and the number of IoT devices the users can experiment with are limited. What is more, in an actor-based IoT middleware, developers can be provided with different kinds of IoT devices, scattered around the network, to experience the plug and play capabilities of the IoT.

In the last couple of years, according to the work in [29], many middleware platforms have been proposed that differentiate depending on their architecture, the level of programming abstractions, and implementation domains. A well-known service-based IoT middleware developed for building automation, healthcare, and agriculture scenarios is Hydra [30]. Another widely used cloud-based IoT middleware's platform is Xively [31]. Xively aims to provide developers and companies with the ability of integrating all their useful data (collected and produced by physical devices) into other systems in a simple way. Attempts have also been made in the field of autonomous distributed sensor networks to provide efficient middleware solutions, as the one presented in [32]. Moreover, closer to experimental implementation, OpenRemote and Kaa are two well-known and widely used open source middleware platforms. OpenRemote [33] is an open source project aiming to overcome the challenges of integration between many different protocols and solutions available for home automation and offer visualization tools. Kaa [34] is an IoT middleware technology applicable for any scale of enterprise IoT development. It provides a range of features that allow developers to build advanced applications for smart products, flexibly manage their device ecosystems, orchestrate end-to-end data processing, and many more. Furthermore, Calvin [35] is a characteristic example of an open source actor-based middleware by Ericsson. It provides a lightweight programming environment, based on Python, for low energy and memory IoT devices. Calvin represents all entities as actors sharing the same paradigm, making clear the distinction between application development and deployment.

2.3.1. IoT Transformation Using APIs. Middleware and Application Programming Interfaces (APIs) are fundamental enablers of the Internet of Things. APIs act as a standard gateway for device communication. They can be used for device registration and activation, providing a management interface for the sensors and exposing a device capability. APIs are going to play a key role in growing the IoT capabilities, as they provide the standard way of communication between devices and sensors. IoT defines that everything and everyone will be accessible as a virtual resource on the Web. In light of this assumption, novel applications that are created out of existing capabilities are going to emerge [41]. This is the basis of the desired automation provided by the IoT, to be applied at home and industry environments. The smart home use case includes the development of the most common and already growing software defined applications. Muzzley [42], Insteon [43], and Indigo Domestics [44] are some well-known third-party providers in this field.

Muzzley offers the ability to develop applications in an Internet of Things platform including features related to lighting, thermostats, automotive, and health. The Muzzley REST API provides automation, while connecting and controlling the devices involved. This API also requires API Keys for authentication and exchanges information in JSON format. In addition, Muzzley offers advice on building and interacting with connected devices. On the same page, Insteon is a home automation system that allows users to automate various functions at home, such as lighting, power outlets, and wall switches. The Insteon API provides access to the functionality of Insteon with other applications and enables the creation of new applications. Some example API methods include managing accounts and account information, managing devices, and setting controls for devices. Regarding Indigo Domotics API, abilities of monitoring and controlling smart home devices into third-party applications are provided. Based on this API's scheduling and triggers, users can not only control their smart homes but also automate them. Indigo Domotics supports many popular smart devices, and users can customize its graphical user interface to their liking. Last but not least, Zetta [45] is an open source platform that combines REST APIs, WebSockets, and reactive programming. It is most suitable for assembling multiple devices into data-intensive, real-time applications.

The ongoing evolution of the IoT and corresponding API ecosystem will optimize APIs based on infrastructure perspective and ensure the availability of control points over the newly generated, inferred, and shared data.

2.3.2. IoT Application Programming Tools. An IoT application combines different software elements that communicate with each other by using Internet protocols and standards. These components are sensing or actuating devices, a gateway device for enabling the connectivity between the short range and the wide area network, a user interface device for interaction with the IoT application, and a Web component to provide connection with the cloud infrastructure [46]. A number of IoT platforms and tools can be utilized by application providers and new developers in deploying and operating their applications and services [46]. However, in this section, we will only focus on a few of them.

Node-RED [47] is an IBM programming tool for connecting hardware devices, APIs, and online services. It provides a browser-based flow editor with a well-defined visual representation that facilitates the composition of IoT devices. Node-RED is built on Node.js, providing event-driven programming and nonblocking features. The flows created in

Node-RED are stored using JSON which can be easily imported and exported for sharing with others.

A similar integration platform for the IoT is ioBroker [48] that is focused on building automation, smart metering, ambient assisted living, process automation, visualization, and data logging. IoBroker defines the rules of data exchanged and published events between different systems. In light of simplifying building efficient and modern serverless functions and edge microservices, the Project Flogo was created, as an event-driven open source framework [49]. The most important asset of Flogo is its ultralight process engine, while providing elegant visuals for apps and frameworks development. Eclipse has also provided an extensible open source IoT Edge Framework based on Java/OSGi, named Kura. Kura [50] offers API access to the hardware interfaces of IoT Gateways and includes already formed protocols, like Modbus. This platform provides a Web-based visual data flow programming tool in order to acquire data from the field, process it at the edge, and publish it to leading IoT Cloud Platforms through MQTT connectivity.

According to the kind of application and use of specific sensing equipment, the chosen programming tool may vary. Some of these tools are even specifically developed for experimentation by amateurs in order to develop an innovative idea in the market. Nevertheless, they offer professionals full access on equipment and advanced programming abilities for research purposes.

2.3.3. IoT Industrial Initiatives. IoT programming tools and application frameworks are intertwined with existing industrial device initiatives. In IoT application development platforms, device connectivity is enabled mostly via preinstalled APIs, software agents, libraries, and toolkits. As for network connectivity for the devices, it could be implemented via cellular or satellite connections, with a fail-over connection option. Furthermore, many platforms are supporting directly plugged certified devices with the according firmware. Nowadays there is a wide variety of hardware development boards and prototyping kits in the market, facilitating the development of IoT applications. Microcontroller development boards are printed circuit boards performing data processing, storage, and networking, onto a single chip. Based on these boards, smart objects are represented with a combination of sensors and actuators imported.

Arduino [51] is an open source hardware and software platform that designs development boards and tools to support digital devices. Arduino board designs use a variety of microprocessors and controllers. Arduino Uno, Espressif Systems ESP8266 [52], and Particle Electron [53] are Arduino-compatible microcontrollers. As far as programming is concerned, Arduino-compatible microcontrollers are based on C or C++ and the provided Arduino IDE. However, other visual programming tools and language bindings can be used. Optionally, Arduino-compatible boards can also support shields, so as to add network or Bluetooth connectivity to a device that is lacking this ability [54]. Smart object development can also be supported by Single Board Computers (SBCs). SBCs are more advanced than microcontrollers, offering more memory and processing power. They also support the attachment of peripheral devices. Three most basic SBCs are the Raspberry Pi 3 Model B [55], BeagleBone Black [56], and DragonBoard 410c [57]. Last but not least, NXP is another well-known provider of applications development boards, like Wandboard and RIoTboard. These boards are low-cost, computer-on-modules with operating systems allowing fully embedded application development with the capabilities of a computer without drawbacks (cost, size, robustness, noisy fan, etc.) [58]. All necessary interconnections are also available: Ethernet, HDMI, USB, WiFi, SATA, and PCIe.

IoT application projects cover a huge variety of experimental fields, as already presented in a previous section. In order to support the according applications IoT devices are designed with detailed and specific knowledge to serve in demanding and special environments. There is no one-size-hardware that can fit all IoT projects. That is the basic lesson of prototyping and experimentation with microcontrollers and SBCs, towards the deployment of completely custom components tailored to the developers' needs. The middleware is a basic architectural layer of the IoT infrastructure implementing the smart decision making and general management between the interconnected devices. Figure 3 presents a taxonomy concerning the middleware's composition and architecture.

2.4. IoT Architecture. A generic IoT architecture includes three layers: application, transport, and sensing [59, 60]. However, a more detailed architecture is usually adopted where five layers are defined [4]:

(1) Perception layer: also known as the 'Device Layer'. Sensor devices and physical objects belong in it

(2) Network layer: aso known as 'transmission layer'. It is responsible for securely transferring data from sensing devices to the information processing system

(3) Middleware layer: responsible for service management and provision of interconnection to the system database. It receives data from the network layer and stores it to the database. This layer processes information, performs ubiquitous computations, and makes automatic decisions based on the outputs

(4) Application layer: provides global management of the provided applications considering the objects information which was processed in the Middleware layer

(5) Business Layer: responsible for the management of the whole IoT system, including services and applications

Several IoT standards have been introduced to facilitate and simplify the programming tasks and operations towards developing applications and services. The work in [7] summarizes the most outstanding protocols defined. Table 2 presents the standardization efforts in IoT support. In the light of the remarks of these standardization efforts, in our work we emphasize the networking technologies of IoT and present a taxonomy of existing technologies.

Table 2: Standardization efforts in IoT support.

Infrastructure Protocols	Routing Protocol	RPL			
	Network Protocol	6LoWPAN		IPv6	
	Link Layer	IEEE 802.15.4			
	Physical Layer	LTE - A	IEEE 802.15.4	EPC global	Z-Wave

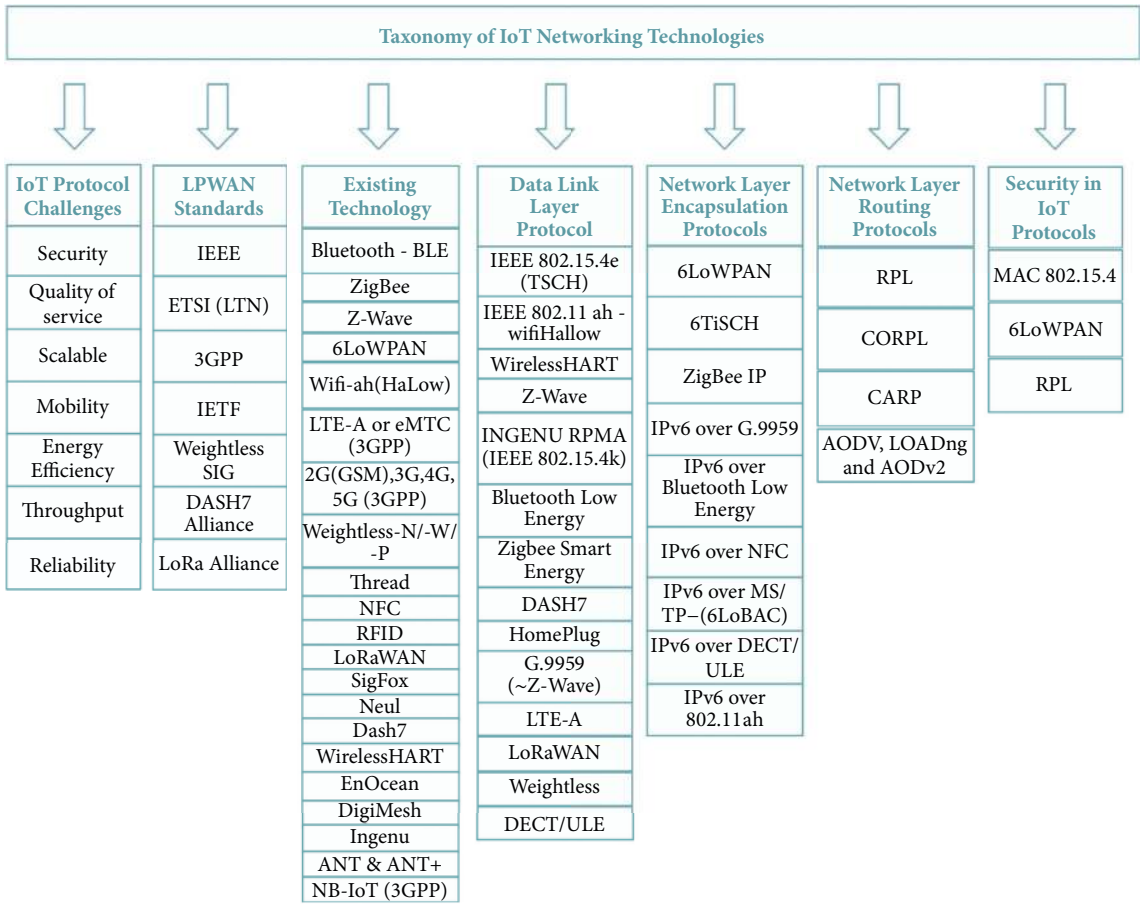

Figure 2: Taxonomy of IoT technologies.

3. IoT Technologies

The IoT vision can be supported by a variety of exciting technologies for different kinds of applications. This section is dedicated to presenting and compiling the most appropriate IoT technologies. Figure 2 summarizes the compiled IoT technologies aiming at presenting each technology aspect and qualification based on an architectural point of view. IPv6 protocol offers many benefits to IoT development and infrastructure. These include unicast, multicast, mobility support, address scope, and autoconfiguration [61]. In the following, the compiled technologies are presented:

(i) Bluetooth Low Energy (BLE) [62]: BLE, known as Bluetooth Smart, part of the Bluetooth v4.0 and the recent v4.2 stack, is a global personal area network protocol built for transmitting small data pieces infrequently at low rates with significantly low power consumption per bit. It constitutes a lightweight version of the classic Bluetooth destined for low energy resource-limited devices. BLE provides many benefits over its competitors; however, it is not an open wireless technology standard and does not support open firmware and hardware

(ii) ZigBee [63]: ZigBee is a short-range radio communication standard for embedded devices and constitutes a mesh Local Area Network (LAN) protocol, initially developed for building control and automation. Similarly to Bluetooth, ZigBee has a large installed operation base, although probably more in industrial deployments. It exhibits some notable benefits in complex systems offering low energy functionality, advanced security, robustness, and high scalability with large amounts of nodes and is well positioned to exploit sensor networks and wireless control in IoT

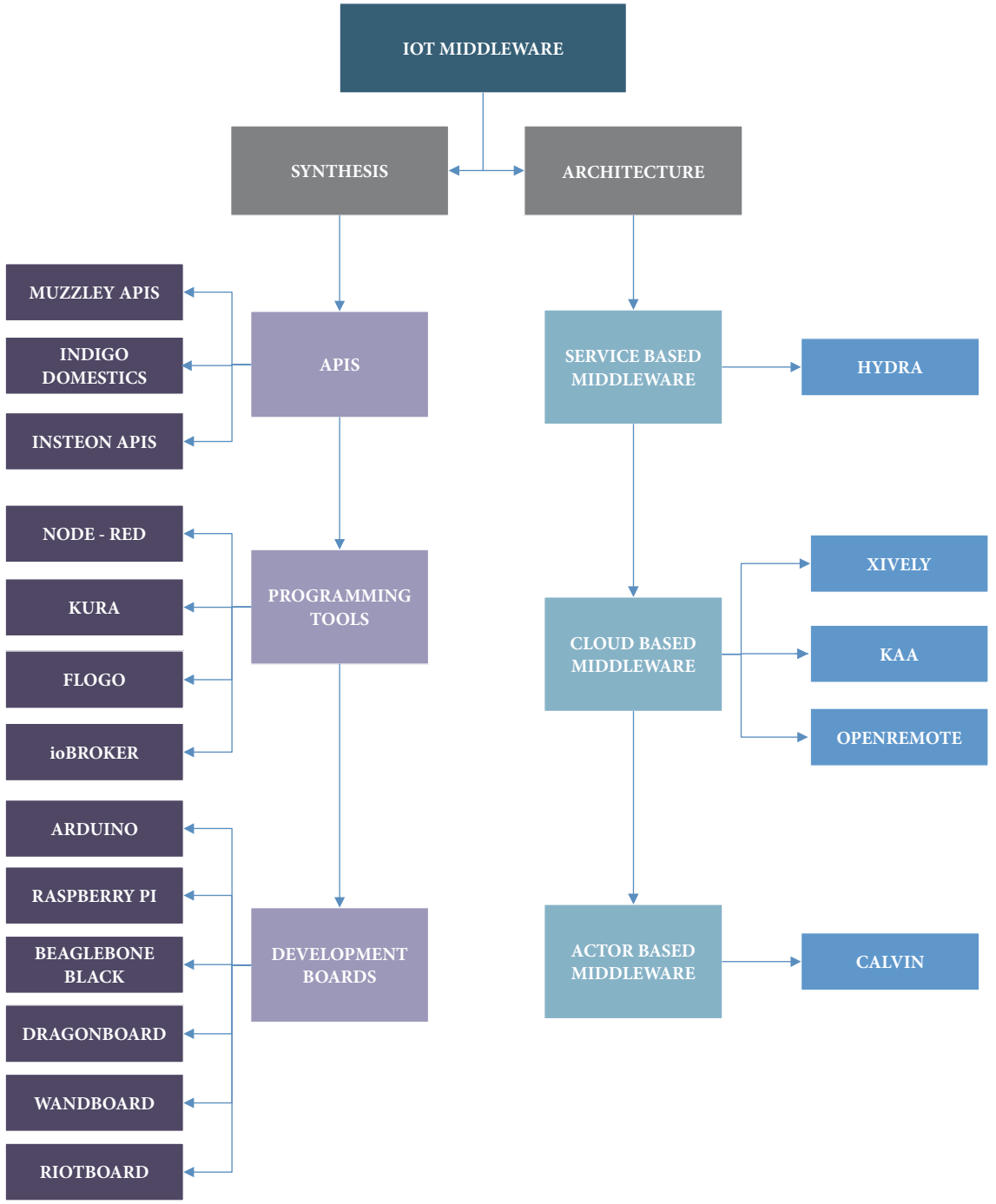

Figure 3: IoT Middleware Architectural Taxonomy.

and M2M applications. The most recent version of ZigBee is the lately launched v3.0, which is actually the integration of various ZigBee standards into a single unified standard

(iii) Z-Wave [10]: Z-Wave is a low energy Radio Frequency (RF) technology for sub-GHz communications. It is a mesh networking protocol, often adopted for home automation, security systems, and lighting controls. Z-Wave employs a simpler protocol than some other alternatives, which allow faster and simpler development. It also supports full mesh networking without requiring a coordinator node and is highly scalable. It operates on 900 MHz with 9.6/40/100 kbit/s data rates

(iv) IPv6 over Low Power Wireless Personal Area Network (6LoWPAN) [8]: 6LoWPAN is defined for devices that are IEEE 802.15.4 compatible and efficiently encapsulate IPv6 long headers in IEEE 802.15.4 small frames. The standard is independent of the

underlying physical layer and frequency band and can be also employed over different communications platforms, including Ethernet, 802.15.4, Wifi, and sub-1 GHz ISM (Industrial, Scientific, and Medical) radio channels. Especially developed for building and home automation, IPv6 offers the fundamental transport scheme to create complex control systems and to connect with devices cost-effectively via a low energy wireless network

(v) WiFi-ah (HaLow) [64]: It is devised specifically for low capacity, long-range sensing devices and controllers. Wifi Alliance has proposed Wifi HaLow as the designation for products supporting the IEEE 802.11ah technology. The protocol is intended to be competitive with Bluetooth 5 with its low energy consumption, but with a large range of coverage. Wifi HaLow supports radio channels below one gigahertz and extends Wifi into the 900 MHz band. The specific technology provides interoperability across multiple vendors, strong government-grade security, and simple deployment

(vi) LTE-A [65]: LTE-A is standard for mobile communications and a significant enhancement of the LTE standard, by focusing on higher capacity. The improvements of LTE-A compared to LTE concern the enhancement of spectral efficiency and network capacity as well as the power efficiency and the operator cost reduction. The main technical elements that make LTE and LTE-A more superior than 3G technologies are the efficient adoption of Orthogonal Frequency Division Multiple Access (OFDMA) in combination with smart antennas supporting Multiple-Input Multiple-Output (MIMO) in the uplink and downlink directions. Another notable aspect of the abovementioned technologies is the new strategy of deployment over heterogeneous networks

(vii) Second-Generation (2G) Global System for Mobile (GSM) [66]: GSM is a global system for mobile communications. It is used to describe the protocols for 2G digital cellular networking employed by mobile phones. It is characterized as a circuit switched technology which is designed for full-duplex voice telephony. GSM is based on Time Division Multiple Access (TDMA) spectrum sharing. GSM supports five cell sizes, namely, fento-, pico-, micro-, macro-, and umbrella cells. The corresponding networks operate in the 900 MHz or 1800 MHz bands

(viii) Third-Generation (3G) and Fourth-Generation (4G) standards [66]: 3G was the first 'high rate' cellular network, while it constitutes an umbrella of standards that refer to a number of technologies which meet the IMT-2000 specifications. Email, web browsing, picture sharing, video downloading, and other smartphone technologies appeared in the third generation. Two key standards for 3G mobile networks are the Universal Mobile Telecommunication System (UMTS) and Code Division Multiple Access 2000 (CDMA2000). 3G networks are capable of providing around 2 megabits per second (basic version)

(ix) Fourth-Generation (4G) [66]: the family of cellular standards that followed 3G formed 4G and is the most popular technology used nowadays for mobile cellular data. According to the respective specifications, the supported data rate of a related standard has to be at least 100 Mbps and up to 1 Gbps to pass the 4G requirements. It is also required to distribute network resources efficiently to support an increased number of simultaneous connections in the cell. The actual range 4G networks was limited to large metropolitan areas. Outside of these areas, 4G phones usually regress to 3G standards

(x) Fifth-Generation (5G) [66]: 5G is destined to be the next generation of cellular network standards, aiming at higher throughput and lower latency. The realization and wide deployment of 5G protocols is set around the year of 2020. 5G is intended to provide wireless communications with almost no restrictions, sometimes called "REAL wireless world". It is said to contain wearable devices with AI capabilities and High Altitude Stratospheric Platform Station (HAPS) systems

(xi) SigFox [10, 67]: SigFox is a global IoT network operator, which is positioned between WiFi and cellular in terms of coverage. It operates in the ISM bands of 900 MHz and utilizes the Ultranarrow Band (UNB) technology. It is designed to handle solely low data rates of 10 to 1,000 bps. SigFox deployments includes antennas on towers (similar to a cell telephony operator) and receives data transfers from devices such as water meters and parking sensors. SigFox is a very promising candidate for applications where the networks only needs to handle small amount, infrequent bursts of information. However, sending data back to the sensors/devices (downlink capability) is severely limited and signal interference can become an issue.

(xii) Weightless-N [67]: Weightless-N is classified as a UNB standard supporting only one-direction communications from end devices to a base station, achieving notable power conservation and reduced cost compared to alternative WEIGHTLESS schemes. Weightless-N is an unlicensed spectrum narrowband protocol which is quite similar to SigFox, but it exhibits better MAC layer implementation. Weightless-N is the only truly open standard that operates in sub-1 GHz unlicensed spectrum

(xiii) Weightless-W [67]: Weightless-W is intended to operate in TV White Space (TVWS) bands as an open standard. It can function under several modulation schemes, including Differential-BPSK (DBPSK) and 16-Quadrature Amplitude Modulation (16-QAM). According to the link budget, the packets which are larger than 10 bytes can be transferred at rates between 1 kbps and 10 Mbps. However, the ability to share networks within the TV white spaces is allowed

only in specific regions; thus, WEIGHTLESS-SIG sets two more standards in ISM bands, which are widely available for unlicensed use

(xiv) Weightless-P [67]: Weightless-P is the most recent technology classified as "Weightless". It provides blended two-direction connectivity with two nonproprietary physical layers. It performs signal modulation utilizing Quadrature Phase Shift Keying (QPSK) and Gaussian Minimum Shift Keying (GMSK). It operates in sub-GHz ISM bands and each single 12.5 kHz narrow channel provides capacity between 0.2 kbps to 100 kbps. However, it has limited hardware availability and communication range

(xv) Thread [10]: Thread builds on the 6LoWPAN and IPv6 protocols as an open standard. It is aimed at the home automation environment. Basically, it as Google's version of ZigBee. Unlike Bluetooth or ZigBee, Thread is not an IoT applications protocol. It is mainly developed as a complement to Wifi, which is sufficient for many end devices but has weaknesses when used for home automation. Mesh networking through IEEE 802.15.4 radio interfaces is supported by Thread, and it is able to handle up to 250 devices with advanced encryption and authentication

(xvi) NFC [10]: NFC enables radio communication between smartphones and portable devices by touching each other or bringing them into short proximity (typically less than 10 cm). NFC operates on 13.56 MHz (ISM) with 100-420 kbps data rate

(xvii) RFID [12]: radio frequency identification utilizes radio signals to monitor and identify in real-time objects or people without requiring line-of-sight communication. This protocol was designed aiming at allowing devices without batteries sending a signal. An RFID system includes a reader, a tag, and a host. A microchip is located in the tag and communicates over a wireless connection using different frequencies in the LF (Low Frequency), HF (High Frequency), or UHF (Ultrahigh Frequency) bands. Tags are typically read-only passive devices, without processing capabilities. RFID tags are used for shipping and tracking purposes

(xviii) LoRaWAN [67, 68]: LoRaWAN is classified as a Media Access Control (MAC) protocol which is built to support public networks of large scale with a single operator. LoRa is the physical layer, i.e., the chip. Also, it spreads out data on various radio channels and transmission rates employing coded messages, instead of adopting narrowband transmission. LoRaWAN considers that devices have varying capabilities depending on their respective application requirements. Thus, three classes of end devices are defined by LoRaWAN, with all of then supporting duplex communication, but with varying energy requirements and downlink latency

(xix) Neul [10]: Neul is similar to SigFox while it operates in the sub-1 GHz band. As a result, it manages to leverage very short bands of the TVWS spectrum to provide high coverage, high scalability, low-cost, and low power wireless networks. Its communications technology is Weightless. The provided capacity can range from a few bps up to 100 kbps using the same single connection. Devices can use 2xAA batteries to consume as little as 20 to 30 mA, corresponding to 10 to 15 years energy autonomy

(xx) Dash7 [67]: Dash7 is an open source protocol for wireless networking with a huge RFID contract with the US Department of Defense. It uses two-level Gaussian Frequency Shift Keying (GFSK) as narrow band modulation scheme in sub-GHz bands. DASH7 is designed to use by default a tree topology, with the alternative to opt for a star layout. It also includes a full network stack, which allows end devices and applications to communicate with one another without the need to address the complexities of the underlying MAC or physical layers. DASH7 also supports symmetric key cryptography and forward error correction

(xxi) WirelessHART [69, 70]: WirelessHART is designed over the HART Communication Protocol. In essence, it constitutes the "industry's first international open wireless communication standard". It adopts a self-healing, self-organizing, and time synchronized mesh architecture. WirelessHART uses IEEE 802.15.4 standard radios and operates in the 2.4 GHz ISM band

(xxii) EnOcean [71]: EnOcean is a protocol built specifically for extremely low power energy harvesting applications. It operates in the bands of 315 MHz in North America and 868 MHz in Europe. The transmission coverage extends up to 30 meters indoors and up to 300 meters outdoors

(xxiii) DigiMesh [72]: DigiMesh is a proprietary protocol for mesh systems. It is designed by Digi as a wireless mesh networking solution that enables low power operation and supports time synchronized sleeping nodes. Contrary to similar protocols like Z-Wave and ZigBee, a unique characteristic of DigiMesh is that all networked devices are of the same type. Every device is capable of routing via a mesh network and sleeping for power optimization. DigiMesh provides various transmission rate alternatives at 900 MHz (10, 125, 150 Kbps) and 2.4 GHz (250 Kbps)

(xxiv) Ingenu [67]: Ingenu was formerly known as On-Ramp Wireless and is a provider of wireless networks. Ingenu owns Random Phase Multiple Access (RPMA), holding 32 patents, and utilizes it for all its network build outs. It uses the free 2.4 GHz ISM bands, while maintaining low power operation. Ingenu was selling metering equipment that collected data from electricity meters at low power. Then, it was rebranded and now it has become a wider player in the respective market sector (like SigFox). Also, Ingenu typically communicates at data rates of

hundreds of thousands of bps, exhibiting increased power consumption compared to LoRa and SigFox

(xxv) ANT & ANT+ [73]: these protocols realize low power proprietary wireless technologies for battery powered applications, such as health monitoring. ANT+ enables the communication of wireless devices from different vendors by presetting specific data payload fields and network parameters and considering device profiles

(xxvi) Narrowband IoT (NB-IoT) [74]: NB-IoT is used for low power devices on cellular M2M. It is based on a Direct-Sequence Spread Spectrum (DSSS) modulation scheme, similarly to the old Neul variant of Weightless-W. NB-IoT operates over 200 KHz radio channels which can be organized within LTE bands, between consecutive LTE channels. The usable bandwidth is 180 kHz with a guard band of 20 kHz, in half-duplex mode at around 200 kbps data rates for the downlink and the uplink. NB-IoT provides data rates similar to LPWA technologies, but with stricter guarantees of achieving them in a stable manner, since it operates in licensed frequency bands

4. Network Protocols for IoT

In this section, the network layer of IoT domain is examined, giving emphasis to encapsulation and routing protocols. Table 3 provides a comparison of the protocol characteristics and their availability.

4.1. Network Encapsulation Protocols

4.1.1. 6LoWPAN. 6LoWPAN protocol is one of the most important schemes in the IoT domain. It is characterized by a special header compression aiming at reducing the transmission overhead, while it entails a fragmentation process to cover the limitation of 128-byte maximum IEEE 802.15.4 frame size. As a result, the total 1280 Bytes of the IPv6 frame [75] (minimum IPv6 Maximum Transmission Unit (MTU)) is fragmented to 127 Bytes, which is the 802.15.4 MTU [76]. The type of each 6LoWPAN packet is determined by the first two bits of the packet. Depending on the type and the following 6 bits (called dispatch field) the details of the remaining structure vary.

6LoWPAN is implemented based on specific types of frame headers. There is the no 6loWPAN header (00), the dispatch header (01), the mesh header (10), and the fragmentation header (11), as shown in Figure 4. If the no 6loWPAN header is absent, frames which are not compatible with the 6loWPAN specifications are dropped. Dispatch header is used for IPv6 header compression and multicasting. Broadcasting is supported via mesh headers, whereas splitting large IPv6 headers into fragments of 128-byte size is enabled using fragmentation headers.

In addition, 6LoWPAN offers interoperability between existing IP devices and low power devices, adopting standard routing schemes [77]. It also leverages a huge body of IP-based management, operations, communication tools, and services.

Regarding security issues, the considered devices may significantly rely on IEEE 802.15.4 link layer mechanisms. IEEE 802.15.4 is based on the 128-bit Advanced Encryption Standard (AES) for encryption and authentication. Furthermore, end-to-end security can be provided either by the IPsec standard or by a mode of Encapsulating Security Payload (ESP) that uses Advanced Encryption Standard-Counter with Cipher Block Chaining-Message Authentication Code (AES-CCM) [76].

4.1.2. ZigBee IP. ZigBee IP is the first open standard protocol that offers seamless Internet connectivity to control low-cost and low power low-cost devices via IPv6-based full wireless mesh networking. ZigBee IP was developed to support ZigBee 2030.5 (previously known as ZigBee Smart Energy 2.0) [36]. Figure 5 presents the ZigBee IP stack which bases its low layer functionality on the IEEE 802.15.4 standard. It uses the header compression techniques of 6LoWPAN to decrease the communication overhead and enhance the network efficiency.

Zigbee IP allows all network nodes to be individually addressed utilizing the IPv6 addressing and routing protocol. A device can operate as a ZigBee Coordinator (ZC), i.e., either as a ZigBee End Device (ZED) or as Zigbee Router (ZR). ZC starts the formation of the network and controls it. ZRs forward data for ZEDs and can be utilized to scale up the network, if necessary. ZEDs are devices of other types participating in the ZigBee network, which are controlled by ZRs and ZCs [12].

Furthermore, Protocol for carrying Authentication for Network Access (PANA) is used for access control to the network, while application security is supported using Transport Security Layer (TLS) 1.2 and elliptic curve cryptography. The application encloses both UDP and TCP messaging protocols available for use.

One of the main benefits of ZigBee IP compared to 802.15.4-based schemes lies in the fact that it offers an expandable architecture using end-to-end IPv6 connectivity. In this manner, ZigBee IP is deemed as a promising asset in leveraging IoT applications.

4.1.3. 6TiSCH. The IPv6 over the TSCH mode of IEEE 802.15.4e (6TiSCH) protocol [78, 79] was created by the IETF 6TiSCH Working Group in order to build and manage the Time Synchronized Channel Hopping (TSCH) schedule for the IEEE 802.15.4e data links. IEEE 802.15.4e [80] is the state-of-the-art solution for reliable and ultralow energy networking for Low Power and Lossy Networks (LLNs). Figure 6 draws the 6TiSCH stack. In a TSCH network, time is sliced into slots and separate communication cells are assigned to unicast or broadcast transmissions at the MAC layer. A number of slot frames constitute a schedule that is being continuously repeated. Schedules indicate to each node what to do in each timeslot based on the following options: (a) transmit, (b) receive, or (c) sleep. The time-slotted operation

Table 3: Characteristics and availability of IoT network protocols.

Encapsulation Technology	6LoWPAN	6TiSCH	ZIGBEE IP	6Lo-G.9959	6Lo-BLE	6Lo-NFC	6Lo-MS/TP	6Lo-DECT/ULE	802.11ah - Wi-Fi HaLow
Data Link Technology	IEEE 802.15.4	IEEE 802.15.4e (TSCH)	Zigbee Smart Energy - IEEE 802.15.4	ITU-T G.9959	Bluetooth LE	ISO/IEC 18000-3 air interface	RS-485 physical layer	DECT ultra low energy PHY	IEEE 802.11ah
Usage	Wide range of applications	Industrial automation	Smart homes, remote controls and healthcare systems	Home automation	Interact/Smart home	Health care Service	District heating - automation networks	Meter reading	Rural communications and offloading cell phone tower traffic
Data Rates	(i) 250 Kbps at 2.4 GHz frequency band (ii) 40 Kbps at 915 MHz frequency band (iii) 20 Kbps at 868 MHz frequency band	Same as in LR-WPANs	Same as in LR-WPANs	According to the RF profile: (i) R1: 9.6 Kbit/s (ii) R2: 40 Kbit/s (iii) R3: 100 Kbit/s	1 Mbit/s at 2.4 GHz frequency ISM band	106 Kbit/s to 424 kbit/s at 13.56 MHz frequency ISM band	115.2 Kbit/s at shielded twisted pair wiring	1.152 Mbit/s symbol rate at 1880 - 1920 MHz frequency band	Up to 347 Mbit/s at 900 MHz frequency band
Mobility	A mobility management mechanism provided depending the application	A mobility management mechanism provided depending the application	A mobility management mechanism provided depending the application	No	Low	Moderate	No	No	No
Topology	Star, P2P and Multihop mesh	Star, P2P and multihop mesh	Star, P2P, cluster tree and mesh	Star, tree and mesh	Star, scatternets and no mesh	P2P and L2-Mesh	Bus and MS/TP	Star and no mesh	Star and no mesh
Security	High and privacy required	High and privacy required	High and privacy required	High and privacy required	Partially	High	High and authentication required	High and privacy required	High and privacy required
Buffering	Low	Low	Low	Low	Low	Low	Low	Low	Low
Latency	High	High	High	High	Low	High	High	Low	High
Applicable Routing protocols	(i) RPL (ii) AODV	(i) RPL (ii) P2P RPL (iii) AODV	RPL	(i) RPL (ii) P2P RPL	RPL	None needed	None needed	RPL	RPL
Advantages	(i) Small packet size (ii) Low bandwidth (iii) Low power (iv) Low cost (v) Location of the devices not predefined (ad-hoc) (vi) Scalability	(i) Large scaling capabilities (ii) High reliability against interference (iii) Low power consumption	(i) Low power (ii) Low cost (iii) Low bandwidth (iv) Scalability (v) Reduces environmental impact (vi) Easy to use (vii) Interoperability specification	(i) Low cost (ii) Low power (iii) Reliability (iv) Real-time applications (v) Collision avoidance mechanisms	(i) Low power (ii) Small battery (iii) Small amounts of data	(i) Simple, quick and safe transactions with a maximum communication speed. (ii) Compatible with existing contactless card infrastructure	(i) Low cost (ii) No mesh, broadcast, or fragmentation headers (iii) Remains the only wired 6Lo PHY (iv) Served as a pattern in formation of the IETF 6Lo working group	(i) Low power (ii) Stable and long range (iii) Two way voice and video (iv) High capacity (v) Long battery life (vi) Interference free	(i) Lower energy consumption (ii) Wide coverage range

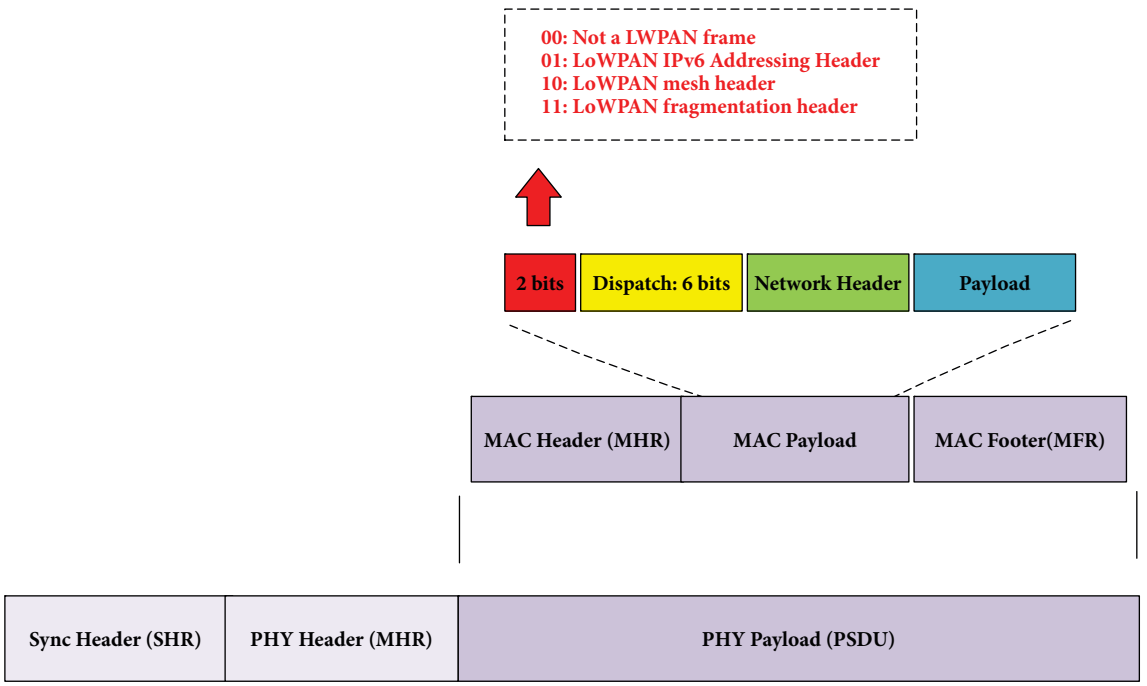

Figure 4: Frame structure in 6LoWPAN.

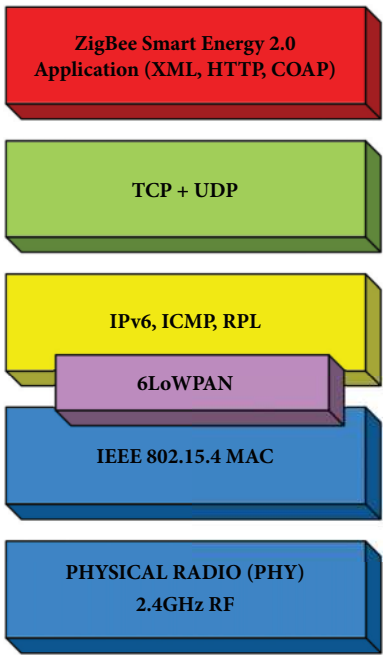

Figure 5: Smart energy 2.0 and ZigBee IP stack [36].

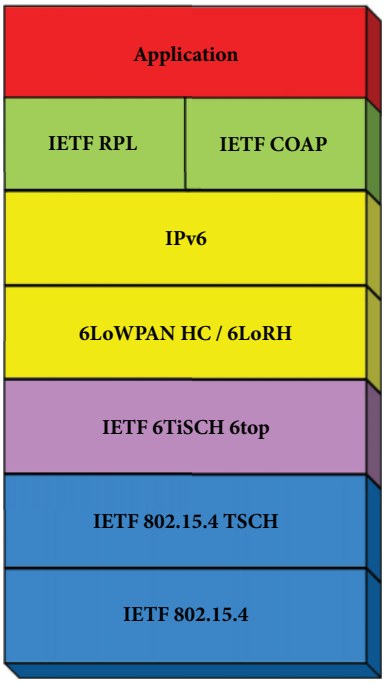

Figure 6: 6TiSCH protocol stack [37].

reduces collisions, allows the usage of various scheduling schemes, and saves energy.

The 6TiSCH Operation sublayer (6top) [37] belongs to the Logical Link Control (LLC), abstracts an IP link over a TSCH MAC, controls the TSCH schedule, collects connectivity information, and monitors the performance of links (cells). The schedule is handled by a channel distribution usage matrix which consists of available timeslots for network scheduling tasks in rows and available frequencies in columns. The resources of this matrix are known to all networking devices.

The 6LoWPAN Routing Header (6LoRH) [81] is employed to compress the IPv6 Routing Protocol (RPL) artifacts

in the IPv6 packets, while 6LoWPAN header compression [82] is utilized to compress the UDP and IPv6 headers. The 6TiSCH architecture defines four ways to manage a schedule, which are combined with three different forwarding models [37]. Furthermore, 6TiSCH uses the general direction of CoAP Management Interface (COMI) for the management of devices combined with the Datagram Transport Layer Security (DTLS) [83]. Regarding security, this architecture expects link layer security combined with a variant of Counter with CBC-MAC (CCM) [84], to be enabled at all times between connected devices.

4.1.4. 6Lo. IPv6 over Networks of Resource-constrained Nodes (6Lo) working group in IETF develops a set of standards on transmitting IPv6 frames over different data links [11]. These nodes are characterized by limited processing, memory and power resources, strict upper limits on state, processing cycles and code space, optimization of network bandwidth and energy usage, and lack of some services at layer 2, such as complete device connectivity and multicast/broadcast. 6Lo working group was formed to cover data links, beyond the IEEE 802.15.4 and IEEE 802.15.4e, which are covered by 6LowPAN and 6TiSCH. Some of these 6Lo specifications that have been approved as RFC [85] are discussed next.

4.1.5. IPv6 over G.9959. RFC 7428 [86] standard sets the frame structure for delivering IPv6 data units in ITU-T G.9959 networks by short-range narrow band digital radio transceivers. Figure 7 illustrates the IP over G.9959 protocol stack. G.9959 networks are divided into domains, which implies that a set of nodes are accessed by the same medium. Each domain is identified by a unique 32-bit HomeID network identifier and contains up to 232 nodes (including the domain master) [87]. The G.9959 HomeID corresponds to an IPv6 subnet which is defined using one or more IPv6 prefixes. Also, an 8-bit NodeID host identifier, which is unique inside the domain, is allocated to each node, instead of a 16-bit short address. An Interface Identifier (IID) is built from a G.9959 link layer address, producing a "link layer IPv6 address", so that it is able to be compressed in G.9959 frame. As for the header compression the format used fits the one applied to IEEE 802.15.4-Based Networks. Moreover, G.9959 involves a Segmentation and Reassembly (SAR) layer for transmitting packets longer than the G.9959 Media Access Control Protocol Data Unit (MAC PDU).

In addition, RFC 7428 uses a shared network key for encryption to offer a level of security. Nevertheless, applications with stricter security demands have to address their authentication and end-to-end encryption employing their own high layer security schemes. Z-Wave is a representative protocol which is based on ITU-G.9959 [87].

4.1.6. IPv6 over Bluetooth Low Energy. RFC 7668 [38] describes the transportation of IPv6 over the connections of Bluetooth Low Energy (LE), by utilizing 6LoWPAN specification model. The IPv6 and Protocol Support Service (IPSS) on the Bluetooth LE stack is drawn in Figure 8. According to the standard's protocol stack, the higher layer includes the

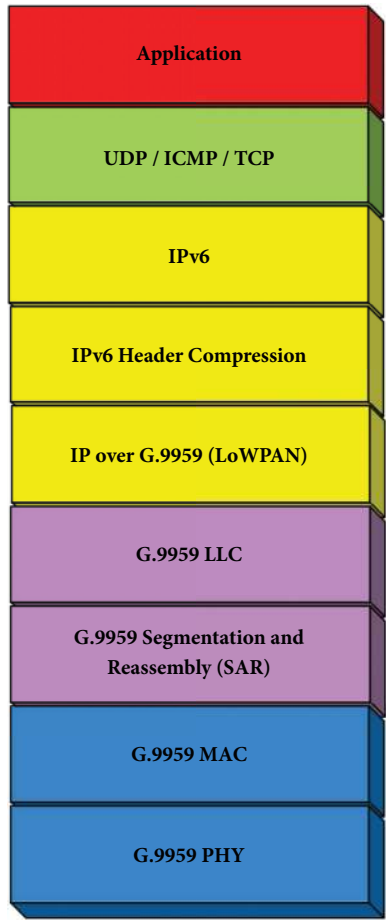

Figure 7: IP over G.9959 protocol stack.

Logical Link Control and Adaptation Protocol (L2CAP), the Attribute Protocol (ATT), and the Generic Attribute Profile (GATT). All Bluetooth smart devices use the GATT that consists of a client, a server, a data value that is transferred, a service, and a descriptor of the characteristic value. Moreover, the Host Controller Interface (HCI) comes between the lower layers, while the L2CAP sublayer is responsible for multiplexing the data channels from the layers above. Moreover, it enables fragmenting and reassembling long data packets.

In Bluetooth LE, there is a direct wireless connection only between a peripheral and a central device. A device in the central role can manage different concurrent connections with several peripheral devices. A peripheral is typically connected to a single central, but it can also communicate with multiple centrals simultaneously. Two peripherals are able to communicate through the central by adopting IP routing according to the respective specification.

Bluetooth LE technology sets restrictions on the size of the protocol overhead in order to satisfy low energy consumption. However, fragmentation techniques from 6LowPAN standards are not adopted, since the L2CAP sublayer already allows segmentation and reassembly of longer data units into 27 byte L2CAP packets. One more notable variation is that Bluetooth LE is not currently able to form multihop

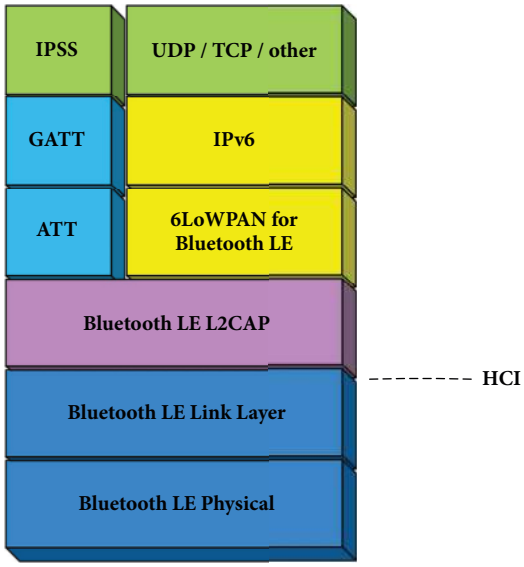

Figure 8: IPv6 on the Bluetooth LE Stack [38].

link layer networks. As an alternative, a central node routes data among lower-powered peripheral devices. So, peripheral and central devices will operate as a 6LoWPAN Border Router (6LBR) and a 6LoWPAN Node (6LN), respectively. Nevertheless, interperipheral data exchange over the central domain is realized by adopting IP routing functionality according to the respective specification.

The Internet Protocol Support Profile (IPSP) that includes the IPSS allows finding devices supporting the IPv6 protocol and establishing link layer connectivity for delivering IPv6 datagrams. Regarding security considerations, Bluetooth LE provides authentication and encryption in the link layer by adopting the Counter with CBC-MAC (CCM) technique and an AES block cipher. This feature, if available, can also be used in higher layers.

4.1.7. IPv6 over NFC. In NFC there is always an initiating devices and a target device, where the initiator actively creates a radio frequency field which is able to power a passive target. NFC extends the functionality of RFID systems by enabling bidirectional communication between the devices, where past techniques, like contactless smart cards, were just unidirectional. Figure 9 illustrates the protocol stack for IPv6 over NFC [88]. In higher layers, transport protocols (UDP and TCP), application protocols, and other protocols are included being able to run over IPv6.

The Logical Link Control Protocol (LLCP) contains the LLC and coordinates the MAC multiplexing mechanisms. Based on multiplexing procedures, existing wireless protocols are integrated into the LLCP formation, while LLC includes three individual components, i.e., the link management, the connection-less transport, and the connection-oriented transport.

6LoWPAN standards provide the configuration of IPv6 address, neighbor discovery, and header compression for decreasing overhead that can be applied to NFC, through the adaptation layer. In order to communicate data NFC in IPv6, an IPv6 datagram passes down to the LLCP of NFC and gets delivered through the Protocol Data Unit (PDU) of LLCP of the NFC-enabled peer device. The LLCP will transfer the Source Service Access Point (SSAP), that is, a 6-bit identification, representing a type of Logical Link Control address, and the DSAP (LLC address of the destination NFC-enabled device) value to the IPv6 over NFC protocol.

Due to the limited RF distance, secure transmissions of IPv6 packets can be arranged, if each individual NFC connection is able to utilize a new short address with a connection limited in duration. In this manner, address scanning can be mitigated, along with device-specific vulnerability exploitation and location tracking.

4.1.8. IPv6 over MS/TP (6LoBAC). Master-Slave/Token-Passing (MS/TP) is a widely used data link protocol defined in BACnet, based on RS-485 single twisted pair PHY [89]. It contains a contention-free MAC and is considered as a wired alternative to IEEE 802.15.4. Devices based on MS/TP usually contain a microcontroller with low memory, processing power, and small cost. An MS/TP interface just needs a Universal Asynchronous Receiver-Transmitter (UART), an RS-485 transceiver, and a 5 ms resolution timer. A token is used in MS/TP to manage access to the multidrop bus. The unsolicited data transfer can only be initiated by a MS/TP master node holding the token. The token is passed to the following master node (according to its MAC address), after the current master node sends at most a predefined maximum number of data units.

RFC 8163 identifies the frame structure for transmitting IPv6 datagrams and the technique for setting link-local and autoconfigured IPv6 addresses on MS/TP networks. MS/TP is notably different than 6LoWPAN in at least three aspects: (a) MS/TP devices are usually powered by the mains; (b) all MS/TP devices within the same segment have direct connectivity; hence, there are no mesh routing or hidden node problems; and (c) the most recent MS/TP specification supports long payloads, removing the requirement of fragmenting, and reassembling below IPv6.

MS/TP devices are always in reception mode and can receive and acknowledge wireless messages. At the same time, they can act as routers for other devices. Nevertheless, all devices that handle MS/TP power (switches and blind controls) are typically MS/TP powered because they are connected to the MS/TP power signals anyway [90].

On the other hand, 6LoBAC is a new frame type for IPv6 Encapsulation that includes a header compression mechanism and improves MS/TP link utilization. According to the LoBAC encapsulation format, which describes the MSDU of an IPv6 over MS/TP frame, the LoBAC payload follows the encapsulation header stack. Also, the IPv6 link-local address for an MS/TP interface is created by adding the interface identifier. Regarding the security considerations, we can infer that these globally visible addresses (the MAC-address-derived interface identifiers) make the network vulnerable to address-scanning attacks. Thus, it is suggested that a 64-bit semantically opaque interface identifier should be created for every globally visible address.

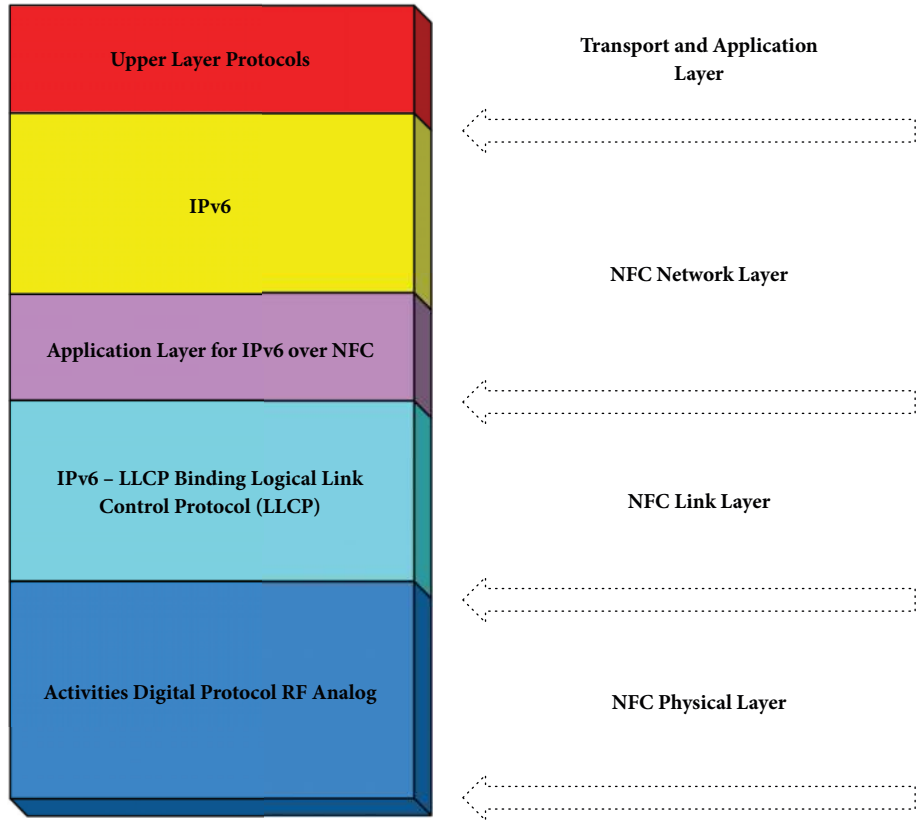

Figure 9: Protocol Stack for IPv6 over NFC.

4.1.9. IPv6 over DECT/ULE. Digital Enhanced Cordless Telecommunications (DECT) Ultralow Energy (ULE) [91] is introduced by the DECT Forum as a low energy air interface technology and is specified and defined by the European Telecommunications Standards Institute (ETSI). DECT ULE intends to offer low bandwidth in smart sensor devices towards automation at home. RFC8105 [39] defines how to map IPv6 above DECT ULE, as demonstrated in [38, 76, 82, 92]. According to the DECT ULE Protocol Stack, as illustrated in Figure 10, MAC layer supports the traditional DECT circuit mode operations and a new ULE packet-mode operation. To this end, the DECT ULE Data Link Control (DLC) supports multiplexing, segmenting, and reassembling for long packets from the higher layers. It also implements per-message authentication. 6LoWPAN standards provide configuration of IPv6 addresses, neighbor Discovery processes, and header compression for reducing overhead.

Data transmission over DECT ULE is established by a Permanent Virtual Circuit (PVC), set between the FP (DECT Fixed Part or the Gateway) and the PP (DECT Portable Part or 6LN) coordinated by a DECT service call. Once the connection of the FPs and PPs is set, the IPv6 address configuration and data exchange can be initiated. The link is now considered to be active.

DECT ULE provides security in the link layer in the form of encryption and message authentication based on Counter with Cipher Block Chaining-Message Authentication Code (CBC-MAC) mode similar to [84]. Encrypting and authenticating messages are again based on AES128. During the establishment of DECT ULE a master User Authentication

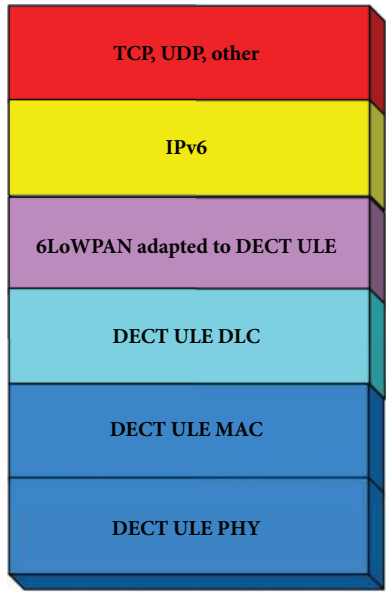

Figure 10: IPv6 over DECT ULE Stack [39].

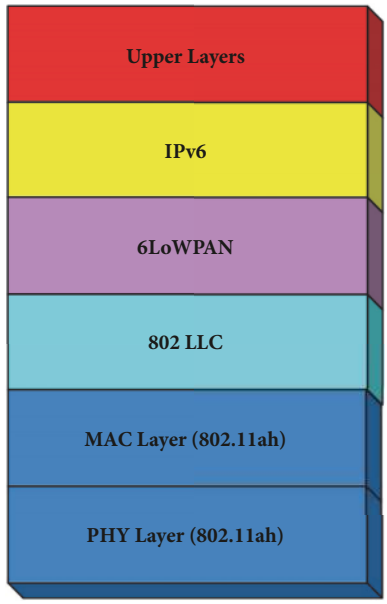

Figure 11: Protocol Stack for IPv6 over 802.11ah [40].

Key (UAK) is produced. Both the session security key and the master authentication key are created by executing the DECT Standard Authentication Algorithm #2 (DSAA2) algorithm, which uses AES128 as the underlying algorithm.

4.1.10. IPv6 over 802.11ah. IEEE 802.11 is widely deployed Wireless LAN (WLAN) technology that provides wireless connectivity to various devices and is also known as WiFi. The IEEE 802.11ah amendment [40] uses the Sub-1 GHz bands that facilitate and help saving transmission power. It is suitable for IoT by supporting numerous devices on an individual Basic Service Set (BSS) and by providing energy conservation techniques which allow wireless stations to transit from sleep mode to save power.

As 802.11ah is a low power/low-rate technology, the above MAC communication protocols also need to consider energy efficiency. This fact motivates the introduction of 6LoWPAN techniques [76, 82] for effective transmission of IPv6 datagrams over IEEE 802.11ah wireless networks.

The system consists of an Access Point (AP) that establishes BSS and stations (STAs). 802.11ah BSS can involve many associated STAs, with most of the STAs staying in sleeping (dozing) mode most of the time. They can check the transmission of periodic beacon-frames, which include Traffic Indication Maps (TIM). The 802.11ah adopts at layer 2 a star topology, according to which the STAs maintain connectivity to the AP and all communications between STAs go over the AP. IEEE 802.11ah does not support mesh topology at layer 2. The WLAN Protocol Stack consists of the PHY Layer (802.11ah), the MAC Layer (802.11ah), and the 802 Logical Link Layer. IPv6 is compatible with 802.11ah via the LLC, as presented in Figure 11.

Using 6LoWPAN, the nodes, i.e., 6LoWPAN Node (6LN) and 6LoWPAN Border Router (6LBR), are colocated in the same devices having 802.11 properties. Usually, in a 802.11ah star topology, the functionally of 6LBR is provided at the AP. 6LNs are colocated with STAs and communicate with 6LBR via an 802.11ah connection. Since the 802.11ah MAC layer does not define mesh topology, it is implied that the 6LBR is the sole routing device available in the network. Hence, there are no 6LowPAN Routers (6LR). Moreover, considering security issues, the functionalities defined in [76] and its update in [82] can be also assumed valid for the 802.11ah case.

4.2. Routing Protocols. In order to cope with the limitations of the IoT systems, a routing protocol should meet specific requirements and employ different strategies [93]. Such a protocol needs to match the traffic pattern of its deployment area and be resourceful in terms of power consumption. Also, it has to scale in terms of memory and performance, while being able to cope with sparse location changes. Moreover, an IoT routing protocol is required to recognize and avoid one-way links and be conservative on the transmitter energy usage. Last but not least, supporting IPv6 and mobility are considered as essential qualities. The strategies used include proactive routing, by trying to have an global view of the whole network topology at all times, and reactive routing, by searching the routes on demand [94–96]. Table 4 provides a taxonomy of the most important routing protocols in IoT domain.

4.2.1. RPL. In 2012, IETF released a Distance Vector Routing Protocol for Low Power and Lossy Networks (RPL) [97]. RPL creates a Destination Oriented Directed Acyclic Graph (DODAG) which contains just a single path from every leaf node to the root. The whole traffic from the node will be forwarded to the root. The root decides the forwarding of a Destination Advertisement Object (DAO) from a node that needs to communicate. Also, it handles the DODAG Information Solicitation (DIS) requests of nodes that want to join the network. RPL nodes can be either stateless, by keeping tracks of its parents only, or stateful by keeping track of its children and parents.

4.2.2. RPL Enhancements. Various enchantments have been proposed to improve the performance of basic RPL protocol. P2P RPL [98] is a standardized, point-to-point reactive RPL (P2P-RPL) that enables an IPv6 router in a LLN to discover paths to one or more IPv6 routers in the LLN on demand. Enhanced-RPL is an enhancement for RPL protocol aiming at enhancing its reliability. Dynamic RPL (D-RPL) [99] is used for the dynamic applications of IoT. D-RPL improves the energy efficiency of the network and the end-to-end delay and more importantly it adapts to mobility changes better than relevant RPL-based protocols. mRPL [99] is the mobile version of RPL, focusing on the mobility management in IoT environments. However, it neglects other metrics resulting in unneeded handovers and sometimes the establishment of unreliable connections. Furthermore, a "Smarter-HOP" version of mRPL for mobility optimization in RPL was proposed, denoted as mRPL++.

Table 4: Routing protocols in IoT domain: features and characteristics.

Routing protocol name	RPL	P2P-RPL	CORPL	CARP	LOADng
Strategy	Proactive	Reactive	Proactive	Reactive	Reactive
Traffic type	MP2P, P2P & P2MP	P2P	MP2P, P2P & P2MP	MP2P, P2P & P2MP	P2P
Mechanism	Energy-aware metrics & multipath routing	Energy-aware metrics	Energy-aware metrics & multipath routing	Energy-aware metrics & multipath routing	Energy-aware metrics
Algorithm	(i) Distance vector (ii) Source routing	(i) Distance vector (ii) Source routing	Distance vector	Link state	Distance Vector
IPv6 support	Yes	Yes	Yes	Yes	Yes
IoT Routing challenges met	(i) Local and global repairs (ii) Energy usage low (iii) Mobility (iv) High scalability (v) Low memory usage	(i) Local and global repairs (ii) Energy usage low (iii) Mobility (iv) High scalability	(i) Data management (ii) Server technologies	(i) Data management (ii) Storage management	(i) Energy usage low (ii) Mobility (iii) High scalability (iv) Low memory usage
Main features	(i) Loop detection and avoidance (ii) Self-configuration (iii) Timer management	Discovers the best-quality route for any source-destination pair	Opportunistic forwarding approach based on RPL	(i) Link quality selection for packet forwarding (ii) High packet delivery ratio for increasing traffic	(i) A lightweight variation of AODV (ii) Suitable for a more general traffic pattern
Disadvantages	No security	(i) No security (ii) High memory usage	(i) No security (ii) No storage management	(i) No security (ii) No server technologies (iii) No reusability of previously collected data	(i) No security (ii) No local repair (iii) High delay in the route discovery

4.2.3. CORPL. CORPL [100] is a nonstandard extension of RPL that is built for cognitive networks and employs DODAG topology generation. CORPL uses opportunistic data transmission to forward the packet by choosing multiple forwarders (forwarder set). It coordinates them so as to choose the optimal next hop to relay packets to. DODAG is designed similarly to RPL. Every node keeps a forwarding set instead of its parent only and informs its neighbor with its changes using DAG Information Object (DIO) messages. According to the up-to-date information, every node dynamically updates its neighbor priorities so as to build the forwarder set.

4.2.4. CARP. Channel-Aware Routing Protocol [101] is a nonstandard distributed routing protocol used in Underwater Wireless Sensor Networks (UWSNs). Its assets include delivering packets in reasonable time with low energy demands. In addition, it is able to support link quality information that is calculated from historical successful data transfers. The history is collected from adjacent sensors in order to choose the forwarding nodes. The main weakness of CARP is that it does not allow reusing previously gathered data. An enhancement of CARP is denoted as E-CARP [102]. E-CARP allows the sink node to save previously received sensor data. Hence, E-CARP drastically decreases the communication overhead.

4.2.5. AODV, LOADng, and AODVv2. Ad Hoc On-Demand Distance Vector Routing (AODV) [94] is classified as hop-by-hop reactive routing protocol, defined in 2003 by IETF. It employs a Route Request- (RREQ-) Route Reply- (RREP-) cycle that is initiated each time a packet needs to be transferred to an unknown destination. Two successors of AODV are (a) the Lightweight On-Demand Ad Hoc Distance Vector Routing Protocol-Next Generation (LOADng) and (b) the AODVv2. Contrary to AODV which just uses hop-count as a routing metric, its two successors accept various metrics, possibly enabling the use of an energy-aware metric. There are also some other routing protocols that make simplifications on AODV in order to reduce footprint and be well-suited for the dynamic and resource-limited network environment. These are AODVbis, AODVjr, LOAD(ng), LoWPAN-AODV, NST-AODV, and TinyAODV.

5. Open Networking Challenges

Taking into account the IoT market size worldwide, the vast device production, the IoT technology investment, the huge interest in IoT by academia, and the potential return on investment og IoT business, the prospect of IoT technology is expected very bright and high [13]. However, due to the vast scale of the IoT infrastructure with a huge number of devices involved, security challenges will also increase considerably. Security provisioning is necessary in order to disarm malicious actors in threatening the IoT, and, as mentioned through the comparison of protocols in the previous section, it is yet to be met efficiently. The security challenges regarding IoT will continue to constitute a major field of research [13]. Table 5 presents a summary of the open networking challenges in IoT domain.

Beyond security provisioning, another main issue regarding the IoT development is the interoperability between the network protocols. Leading companies worldwide are producing smart devices by taking into account full interoperability capabilities. These capabilities are of paramount importance since they will ensure easy integration with the existing Internet [103]. An IoT protocol designed with many advanced features escalates the cost and lowers the ease-of-use. It is not a trivial task to build an appealing protocol and is typically a tradeoff between the system performance and the cost. IPv6 brings the IoT functionalities one step closer to the desired interoperability introducing useful and applicable networking technologies.

The IoT will interconnect numerous objects to provide innovative services. So, it is required to have an efficient naming and identity management system, which coordinates the unique identities for a large number of objects. One way to create such a system is by using RFIDs, to physically tag one object. Another way is to allow one object with its own description, so that it would be able to directly transmit its own identity and related properties.

This large number of smart objects also leads to the need of better scalability management protocols. As mentioned in [59], existing management protocols cannot be extended efficiently enough to meet the IoT devices' requirements, due to their narrow capabilities.

Furthermore, IoT data are characterized by heterogeneity which means that they are generated in big amounts, they often arrive at real-time, they are variable in terms of structure, and they might be of uncertain provenance. The challenge of handling big data is critical, because the overall performance is in direct proportion to the features of the data management service [104]. This issue becomes even more complicated when the data integrity feature is considered, not only because it affects the quality of service, but also for its privacy and security related issues, particularly on outsourced data [105].

Mobility management is another key issue in the IoT paradigm. The existing mobility-supporting protocols of Mobile Ad Hoc NETworks (MANETs), Vehicular Ad Hoc NETworks (VANETs), and sensor networks are not able to efficiently cope with the typical IoT devices, because of the harsh processing and power limitations. Movement detection is necessary to monitor the device location and respond to topology changes accordingly.

Moreover, the energy requirements in IoT are still not adequately met. As presented previously, some routing protocols support low power communication but they are considered to be in an early stage of development. Hence, green technologies have to be employed, in order to make IoT devices as power-efficient as possible.

6. Discussion and Trends

This paper is focused on the network protocols of IoT. There are many already existing and developing technologies trying to stand up to the challenges of such a vision. However, neither can be considered to be the only appropriate, as the choice depends not only on the application type, but also on

Table 5: Open networking challenges in IoT domain.

loT Open Networking Challenges	Features
Security	(i) Data confidentiality (ii) Identity management privacy (iii) Authentication (iv) Trusted platforms (v) Access control (vi) Encryption
Interopabilty	(i) Need of standardization (ii) Design of predefined specifications of the components (iii) Cross-layer interopability needed (iv) Easy integration with the existing Internet (v) 1Pv6 addressing leading the way
Indetification	(i) Creation of an efficient naming and identity management system
Scalability	(i) Creation of a scalability management protocol for supporting a larger number of smart objects
Big Data	(i) Performance is directly proportional to the properties of the data management service (ii) Data integrity feature should be taken into account
Mobility	(i) VANETs and MANETs should be free of energy and processing constraints (ii) Movement detection needed
Energy Management	(i) Not yet satisfying (ii) Need of green technologies for energy efficient devices

the networks topology and data rate capability. That is why so many standards have already been proposed to match all kinds of physical layers and different relevant technologies, as presented in the previous sections.

More specifically, IoT mainly involves low power network protocols, where IETF 6LoWPAN could be adopted to attach devices to IP networks. These protocols may concern local area, wide area, or personal area networks, as figured through the taxonomy proposed in this paper. With numerous devices entering the Internet space, IPv6 is expected to have a significant role in addressing scalability at the network layer. IPv6 is in fact a fundamental communication enabler for the future Internet of Things. As supported by the IoT6 project, IPv6 is good for IoT and IoT is good for IPv6.

IoT is a highly demanding vision that is yet to be fulfilled and even accepted as a beneficial upcoming technology, due to criticism and controversies regarding privacy, control, and environmental sustainability impact. The research community has to answer to these questions and form a suitable and safe environment for such a huge development. Current trends are focusing on security and privacy issues regardless the level of the architecture. Furthermore, interoperability between technologies has made a few steps.

Another trending challenge involves data management and storage of the huge amount of data to be collected. IoT is trending through the wireless sensor network technologies and takes advantage of all of its assets to deal with the arising problems. Autonomous control and intelligence supported by unique identification through the Electronic Product Code is the desired combination.

All of the networking and routing mechanisms mentioned in the paper are being proposed to improvements and upgrades. Each one of them built with specific qualifications in mind and currently being evaluated in order to meet the IoT requirements, as presented through the protocol tables. For instance, RPL protocol was specifically developed for routing IPv6 frames over low power, lossy networks and is ideal for IoT. However, various types of implementation and alternatives are being developed to cover its faults and be more efficient for different kinds of application.

7. Conclusions

This survey paper was focused on conducting a detailed analysis, comparison, and discussion of qualification on various technologies suitable for the IoT networking platform. Through the proposed taxonomy, each technology's role was presented, based on an architectural point of view of the IoT. More specifically, focus was given on the evaluation and qualification of the suitable network encapsulation and routing protocols. IoT demands interoperability between its technologies. It is a fact that every networking technology that wishes to be involved in this computing paradigm has to receive upgrades like IPv6 compatibility and should also aim to decrease energy consumption. A more crucial requirement is the need for embedded security. Every technology and protocol that was presented in this paper fits some of the basic requirements in order to be used in the IoT. However, their characteristics vary as each one is intended for specific kind of applications and topologies. Through the research conducted to form this paper, the need for security and a better data management system was made quite clear. Nevertheless, proposed protocol enchantments help in filling the gaps of performance in some cases. IoT is the future and strong networking bases need to be set, by improving and upgrading the suitable technologies applied. Our research can serve as a motivation to scholars and professionals towards developing new and more efficient networking protocols, filling current gaps, and dealing with important deficiencies.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] C.-W. Tsai, C.-F. Lai, and A. V. Vasilakos, "Future internet of things: open issues and challenges," *Wireless Networks*, vol. 20, no. 8, pp. 2201–2217, 2014.

[2] D. Miorandi, S. Sicari, F. de Pellegrini, and I. Chlamtac, "Internet of things: vision, applications and research challenges," *Ad Hoc Networks*, vol. 10, no. 7, pp. 1497–1516, 2012.

[3] O. Mavropoulos, H. Mouratidis, A. Fish, and E. Panaousis, "ASTo: a tool for security analysis of IoT systems," in *Proceedings of the 15th IEEE/ACIS International Conference on Software Engineering Research, Management and Applications (SERA '17)*, pp. 395–400, June 2017.

[4] R. Khan, S. U. Khan, and R. Zaheer, "Future internet: the internet of things architecture, possible applications and key challenges," in *Proceedings of the 10th International Conference on Frontiers of Information Technology (FIT' 12)*, pp. 257–260, December 2012.

[5] H. S. Dhillon, H. Huang, and H. Viswanathan, "Wide-area wireless communication challenges for the internet of things," *IEEE Communications Magazine*, vol. 55, no. 2, pp. 168–174, 2017.

[6] V. Gazis, "A survey of standards for machine-to-machine and the internet of things," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 1, pp. 482–511, 2017.

[7] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of things: a survey on enabling technologies, protocols, and applications," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 4, pp. 2347–2376, 2015.

[8] Z. G. Sheng, S. S. Yang, Y. F. Yu, A. V. Vasilakos, J. A. McCann, and K. K. Leung, "A survey on the ietf protocol suite for the internet of things: standards, challenges, and opportunities," *IEEE Wireless Communications Magazine*, vol. 20, no. 6, pp. 91–98, 2013.

[9] L. Mainetti, L. Patrono, and A. Vilei, "Evolution of wireless sensor networks towards the Internet of Things: a survey," in *Proceedings of the 19th International Conference on Software, Telecommunications and Computer Networks (SoftCOM '11)*, pp. 16–21, September 2011.

[10] P. Barker and M. Hammoudeh, "A survey on low power network protocols for the internet of things and wireless sensor networks," in *Proceedings of the International Conference on Future Networks and Distributed Systems (ICFNDS '17)*, pp. 44:1–44:8, New York, NY, USA, July 2017.

[11] T. Salman and R. Jain, *Networking Protocols and Standards for Internet of Things*, John Wiley & Sons, Inc, 2017.

[12] O. Bello, S. Zeadally, and M. Badra, "Network layer inter-operation of Device-to-Device communication technologies in Internet of Things (IoT)," *Ad Hoc Networks*, vol. 57, pp. 52–62, 2017.

[13] B. Javed, M. W. Iqbal, and H. Abbas, "Internet of things (IoT) design considerations for developers and manufacturers," in *Proceedings of the IEEE International Conference on Communications Workshops (ICC Workshops '17)*, pp. 834–839, May 2017.

[14] H. P. E. D. LP, "Internet of things research study," Tech. Rep., 2015, http://files.asset.microfocus.com/4aa5-4759/en/4aa5-4759.pdf.

[15] G. Kortuem, F. Kawsar, V. Sundramoorthy, and D. Fitton, "Smart objects as building blocks for the internet of things," *IEEE Internet Computing*, vol. 14, no. 1, pp. 44–51, 2010.

[16] D. Turgut and L. Boloni, "Value of information and cost of privacy in the internet of things," *IEEE Communications Magazine*, vol. 55, no. 9, pp. 62–66, 2017.

[17] K. Yang, D. Forte, and M. M. Tehranipoor, "Protecting endpoint devices in IoT supply chain," in *Proceedings of the 34th IEEE/ACM International Conference on Computer-Aided Design (ICCAD '15)*, pp. 351–356, November 2015.

[18] P. Sarigiannidis, E. Karapistoli, and A. A. Economides, "VisIoT: a threat visualisation tool for IoT systems security," in *Proceedings of the IEEE International Conference on Communication Workshop (ICCW '15)*, pp. 2633–2638, June 2015.

[19] D. Kandris, G. Tselikis, E. Anastasiadis, E. Panaousis, and T. Dagiuklas, "COALA: a protocol for the avoidance and alleviation of congestion in wireless sensor networks," *Sensors*, vol. 17, no. 11, 2017.

[20] O. Mavropoulos, H. Mouratidis, A. Fish, E. Panaousis, and C. Kalloniatis, "A conceptual model to support security analysis in the internet of things," *Computer Science and Information Systems*, vol. 14, no. 2, pp. 557–578, 2017.

[21] S. McClellan, J. A. Jimenez, and G. Koutitas, *Smart Cities: Applications, Technologies, Standards, and Driving Factors*, Springer International Publishing, 2017.

[22] J. Barbaresso, G. Cordahi, D. Garcia, C. Hill, A. Jendzejec, and K. Wright, "Usdot's intelligent transportation systems (its) its strategic plan 2015-2019," Tech. Rep., 2014.

[23] E. Borgia, "The internet of things vision: key features, applications and open issues," *Computer Communications*, vol. 54, pp. 1–31, 2014.

[24] E. Ancillotti, R. Bruno, and M. Conti, "The role of communication systems in smart grids: architectures, technical solutions and research challenges," *Computer Communications*, vol. 36, no. 17-18, pp. 1665–1697, 2013.

[25] S. Gowrishankar, M. Y. Prachita, and A. Prakash, "IoT based heart attack detection, heart rate and temperature monitor," in *International Journal of Computer Applications*, vol. 170, no. 5, pp. 26–30, Foundation of Computer Science (FCS), New York, USA, 2017.

[26] Z. Li, J. Wang, R. Higgs, L. Zhou, and W. Yuan, "Design of an intelligent management system for agricultural greenhouses based on the internet of things," in *Proceedings of the 20th IEEE International Conference on Computational Science and Engineering and 15th IEEE/IFIP International Conference on Embedded and Ubiquitous Computing (CSE and EUC '17)*, vol. 2, pp. 154–160, July 2017.

[27] I. Lee and K. Lee, "The Internet of Things (IoT): applications, investments, and challenges for enterprises," *Business Horizons*, vol. 58, no. 4, pp. 431–440, 2015.

[28] A. H. Ngu, M. Gutierrez, V. Metsis, S. Nepal, and Q. Z. Sheng, "IoT middleware: a survey on issues and enabling technologies," *IEEE Internet of Things Journal*, vol. 4, no. 1, pp. 1–20, 2017.

[29] M. A. Razzaque, M. Milojevic-Jevric, A. Palade, and S. Clarke, "Middleware for Internet of things: a survey," *IEEE Internet of Things Journal*, vol. 3, no. 1, pp. 70–95, 2016.

[30] M. Eisenhauer, P. Rosengren, and P. Antolin, "A development platform for integrating wireless devices and sensors into ambient intelligence systems," in *Proceedings of the 6th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks Workshops*, pp. 1–3, IEEE, Rome, Italy, June 2009.

[31] Xively, accessed: 2018-07-19, https://xively.com/.

[32] G. Eleftherakis, D. Pappas, T. Lagkas, K. Rousis, and O. Paunovski, "Architecting the IoT paradigm: a middleware for autonomous distributed sensor networks," *International Journal of Distributed Sensor Networks*, vol. 11, no. 12, Article ID 139735, 17 pages, 2015.

[33] Open Source for Internet of Things, "About openremote," accessed: 2018-07-19, http://www.openremote.com/about/.

[34] KAA, "Overview," accessed: 2018-07-19, https://www.kaaproject.org/overview/.

[35] J. Persson, "Open source release of iot app environment calvin," accessed: 2018-07-19, https://www.ericsson.com/research-blog/open-source-calvin/.

[36] M. Franceschinis, C. Pastrone, M. A. Spirito, and C. Borean, "On the performance of ZigBee Pro and ZigBee IP in IEEE 802.15.4 networks," in *Proceedings of the IEEE 9th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob '13)*, pp. 83–88, October 2013.

[37] P. Thubert, "An Architecture for IPv6 over the TSCH mode of IEEE 802.15.4," Internet Engineering Task Force, Internet-Draft draft-ietf-6tisch-architecture-13, Nov. 2017, work in Progress, https://datatracker.ietf.org/doc/html/draft-ietf-6tisch-architecture-13.

[38] J. Nieminen, T. Savolainen, M. Isomaki, B. Patil, Z. Shelby, and C. Gomez, "IPv6 over BLUETOOTH(R) Low Energy," Tech. Rep. RFC 7668, 2015, https://rfc-editor.org/rfc/rfc7668.txt.

[39] P. B. Mariager, J. T. Petersen, Z. Shelby, M. Van De Logt, and D. Barthel, "Transmission of IPv6 Packets over Digital Enhanced Cordless Telecommunications (DECT) Ultra Low Energy (ULE)," Tech. Rep. RFC 8105, 2017, https://rfc-editor.org/rfc/rfc8105.txt.

[40] L. F. D. C. Vega, I. Robles, and R. Morabito, "IPv6 over 802.11ah," Internet Engineering Task Force, Internet-Draft draft-delcarpio-6lo-wlanah-00, work in Progress, https://datatracker.ietf.org/doc/html/draft-delcarpio-6lo-wlanah-00.

[41] M. Vukovic, "Internet programmable iot: On the role of apis in iot: The internet of things (ubiquity symposium)," *Ubiquity*, vol. 2015, no. 3, pp. 3:1–3:10, 2015.

[42] Muzzley, "Integrating with muzzley," accessed: 2018-07-19, https://muzzley.com/documentation.

[43] Insteon, "Insteon," accessed: 2018-07-19, https://www.insteon.com/google-home.

[44] Indigo Domestics, "Home," accessed: 2018-07-19, http://www.indigodomo.com/.

[45] Zetta, "An api-first internet of things platform," accessed: 2018-07-19, http://www.zettajs.org/.

[46] O. Mazhelis and P. Tyrvainen, "A framework for evaluating Internet-of-Things platforms: application provider viewpoint," in *Proceedings of the IEEE World Forum on Internet of Things (WF-IoT '14)*, pp. 147–152, March 2014.

[47] JS Foundation, "Node-red," accessed: 2018-07-19, https://nodered.org/.

[48] ioBroker, accessed: 2018-07-19, http://iobroker.net/.

[49] TIBCO Software Inc, "Flogo project," accessed: 2018-07-19, https://www.flogo.io/.

[50] Eclipse Foundation, "Eclipse-kura," accessed: 2018-07-19, https://www.eclipse.org/kura/.

[51] Arduino Project'S Foundation, accessed: 2018-07-19, https://www.arduino.cc/.

[52] Espressif Systems, accessed: 2018-07-19, https://www.espressif.com/en/products/hardware/esp8266ex/overview.

[53] Particle, accessed: 2018-07-19, https://www.particle.io/products/hardware/electron-cellular-2g-3g-lte/.

[54] A. Gerber, "Choosing the best hardware for your next iot project," 05 2017, accessed: 2018-07-19, https://www.ibm.com/developerworks/library/iot-lp101-best-hardware-devices-iot-project/index.html.

[55] Raspberry Pi Foundation, accessed: 2018-07-19, https://www.raspberrypi.org/.

[56] BeagleBoard.org Foundation, accessed: 2018-07-19, http://beagleboard.org/black.

[57] Qualcomm, accessed: 2018-07-19, https://developer.qualcomm.com/hardware/dragonboard-410c.

[58] NXP, "Community boards," accessed: 2018-07-19, https://www.nxp.com/support/developer-resources/hardware-development-tools/community-boards:COMMUNITY-BOARDS.

[59] I. Yaqoob, E. Ahmed, I. A. T. Hashem et al., "Internet of things architecture: recent advances, taxonomy, requirements, and open challenges," *IEEE Wireless Communications Magazine*, vol. 24, no. 3, pp. 10–16, 2017.

[60] P. Sarigiannidis, E. Karapistoli, and A. A. Economides, "Modeling the internet of things under attack: a G-network approach," *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 1964–1977, 2017.

[61] T. Savolainen, J. Soininen, and B. Silverajan, "IPv6 addressing strategies for IoT," *IEEE Sensors Journal*, vol. 13, no. 10, pp. 3511–3519, 2013.

[62] S. Raza, P. Misra, Z. He, and T. Voigt, "Building the Internet of Things with bluetooth smart," *Ad Hoc Networks*, vol. 57, no. supplement C, pp. 19–31, 2017, special Issue on Internet of Things and Smart Cities security, privacy and new technologies.

[63] P. Rajendhar, P. P. Kumar, and R. Venkatesh, "Zigbee based wireless system for remote supervision and control of a substation," in *Proceedings of the International Conference on Innovative Research in Electrical Sciences (IICIRES '17)*, pp. 1–4, June 2017.

[64] L. F. Del Carpio, P. Di Marco, P. Skillermark, R. Chirikov, and K. Lagergren, "Comparison of 802.11ah, BLE and 802.15.4 for a Home Automation Use Case," *International Journal of Wireless Information Networks*, vol. 24, no. 3, pp. 243–253, 2017.

[65] E. Pateromichelakis, M. Shariat, A. U. Quddus, and R. Tafazolli, "On the evolution of multi-cell scheduling in 3GPP LTE/LTE-A," *IEEE Communications Surveys & Tutorials*, vol. 15, no. 2, pp. 701–717, 2013.

[66] A. Gohil, H. Modi, and S. K. Patel, "5G technology of mobile communication: a survey," in *Proceedings of the International Conference on Intelligent Systems and Signal Processing (ISSP '13)*, pp. 288–292, Gujarat, India, March 2013.

[67] U. Raza, P. Kulkarni, and M. Sooriyabandara, "Low power wide area networks: an overview," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 2, pp. 855–873, 2017.

[68] F. Adelantado, X. Vilajosana, P. Tuset-Peiro, B. Martinez, J. Melia-Segui, and T. Watteyne, "Understanding the Limits of LoRaWAN," *IEEE Communications Magazine*, vol. 55, no. 9, pp. 34–40, 2017.

[69] S. M. Hassan, R. Ibrahim, K. Bingi, T. D. Chung, and N. Saad, "Application of wireless technology for control: A wirelesshart perspective," *Procedia Computer Science*, vol. 105, no. supplement C, pp. 240–247, 2017, http://www.sciencedirect.com/science/article/pii/S1877050917302405.

[70] S. M. Hassan, R. Ibrahim, K. Bingi, T. D. Chung, and N. Saad, "Application of wireless technology for control: A wirelesshart perspective," in *Proceedings of the IEEE International Symposium on Robotics and Intelligent Sensors (IRIS '16)*, vol.

105, pp. 240–247, December 2016, Tokyo, Japan, http://www.sciencedirect.com/science/article/pii/S1877050917302405.

[71] J. Ploennigs, U. Ryssel, and K. Kabitzsch, "Performance analysis of the Enocean wireless sensor network protocol," in *Proceedings of the 15th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA '10)*, pp. 1–9, September 2010.

[72] C. Osiegbu, S. B. Amsalu, F. Afghah, D. Limbrick, and A. Homaifar, "Design and implementation of an autonomous wireless sensor-based smart home," in *Proceedings of the 24th International Conference on Computer Communications and Networks (ICCCN '15)*, pp. 1–7, August 2015.

[73] M. Ghamari, B. Janko, R. S. Sherratt, W. Harwin, R. Piechockic, and C. Soltanpur, "A survey on wireless body area networks for ehealthcare systems in residential environments," *Sensors*, vol. 16, no. 6, 2016.

[74] I. C. R. Tardy, N. Aakvaag, B. Myhre, and R. Bahr, "Comparison of wireless techniques applied to environmental sensor monitoring," SINTEF, p. 19, March 2017.

[75] R. M. Hinden and D. S. E. Deering, "Internet Protocol, Version 6 (IPv6) Specification," Tech. Rep. RFC 2460, 1998, https://rfc-editor.org/rfc/rfc2460.txt.

[76] G. Montenegro, N. Kushalnagar, J. Hui, and D. Culler, "Transmission of IPv6 packets over IEEE 802.15.4 networks," Tech. Rep. RFC 4944, 2007, https://rfc-editor.org/rfc/rfc4944.txt.

[77] G. Montenegro, C. Schumacher, and N. Kushalnagar, "IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals," Tech. Rep. RFC 4919, 2007, https://rfc-editor.org/rfc/rfc4919.txt.

[78] D. Dujovne, T. Watteyne, X. Vilajosana, and P. Thubert, "6TiSCH: Deterministic IP-enabled industrial internet (of things)," *IEEE Communications Magazine*, vol. 52, no. 12, pp. 36–41, 2014.

[79] J. D. R. Nepomuceno and N. M. C. Tiglao, "Performance evaluation of 6TiSCH for resilient data transport in wireless sensor networks," in *Proceedings of the 31st International Conference on Information Networking (ICOIN '17)*, pp. 552–557, January 2017.

[80] "Ieee standard for local and metropolitan area networks–part 15.4: Low-rate wireless personal area networks (lr-wpans) amendment 1: Mac sublayer," IEEE Std 802.15.4e-2012 (Amendment to IEEE Std 802.15.4-2011), pp. 1–225, April 2012.

[81] P. Thubert, C. Bormann, L. Toutain, and R. Cragie, "IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) Routing Header," Tech. Rep. RFC 8138, 2017, https://rfc-editor.org/rfc/rfc8138.txt.

[82] J. Hui and P. Thubert, "Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks," Tech. Rep. RFC 6282, 2011, https://rfc-editor.org/rfc/rfc6282.txt.

[83] E. Rescorla and N. Modadugu, "Datagram Transport Layer Security Version 1.2," Tech. Rep. RFC 6347, 2012, https://rfc-editor.org/rfc/rfc6347.txt.

[84] D. Whiting, R. Housley, and N. Ferguson, "Counter with CBC-MAC (CCM)," Tech. Rep. RFC 3610, 2003, https://rfc-editor.org/rfc/rfc3610.txt.

[85] Y.-G. Hong and C. Gomez, "Use cases for IPv6 over Networks of Resource-constrained Nodes," Internet Engineering Task Force, Internet-Draft draft-hong-6lo-use-cases-01, work in Progress, https://datatracker.ietf.org/doc/html/draft-hong-6lo-use-cases-01.

[86] A. Brandt and J. Buron, "Transmission of IPv6 Packets over ITU-T G.9959 Networks," Tech. Rep. RFC 7428, 2015, https://rfc-editor.org/rfc/rfc7428.txt.

[87] S. G. 15, "Recommendation itu-t g.9959: Short range narrow-band digital radiocommunication transceivers phy and mac layer specifications," Tech. Rep., International Telecommunication Union, 2012.

[88] Y. Choi, Y.-G. Hong, J.-S. Youn, D. Kim, and J. Choi, "Transmission of IPv6 Packets over Near Field Communication," Internet Engineering Task Force, Internet-Draft draft-ietf-6lo-nfc-08, Oct. 2017, work in Progress, https://datatracker.ietf.org/doc/html/draft-ietf-6lo-nfc-08.

[89] K. Lynn, J. Martocci, C. Neilson, and S. Donaldson, "Transmission of IPv6 over Master-Slave/Token-Passing (MS/TP) Networks," Tech. Rep. RFC 8163, 2017, https://rfc-editor.org/rfc/rfc8163.txt.

[90] C. Paetz, "Z-Wave Essentials," Prof. Dr. Christian Paetz, 2017.

[91] ETSI, "Etsi ts 102 939-1: Digital enhanced cordless telecommunications (dect); ultra low energy (ule); machine to machine communications; part 1: Home automation network (phase 1)," ETSI, technical specification, March 2015, http://www.etsi.org/standards-search.

[92] C. Bormann, Z. Shelby, S. Chakrabarti, and E. Nordmark, "Neighbor Discovery Optimization for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)," Tech. Rep. RFC 6775, 2012, https://rfc-editor.org/rfc/rfc6775.txt.

[93] A. Dhumane, "Routing challenges in internet of things," *CSI Magazine*, vol. 03, 2015.

[94] M. Talwar, "Routing techniques and protocols for internet of things: a survey," in *Proceeding of the NCRIET-2015*, pp. 417–423, 2015.

[95] T. B. A. H. Prasad, "Network routing protocols in iot," *International Journal of Advances in Electronics and Computer Science*, vol. 4, no. 4, 2017.

[96] H. Prasad and S. Babu, "A survey on network routing protocols in internet of things (IOT)," *International Journal of Computer Applications*, vol. 160, no. 2, pp. 18–22, 2017.

[97] H.-S. Kim, J. Ko, D. E. Culler, and J. Paek, "Challenging the IPv6 routing protocol for low-power and lossy networks (RPL): a survey," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 4, pp. 2502–2525, 2017.

[98] M. Zhao, A. Kumar, P. H. Joo Chong, and R. Lu, "A comprehensive study of RPL and P2P-RPL routing protocols: Implementation, challenges and opportunities," *Peer-to-Peer Networking and Applications*, vol. 10, no. 5, pp. 1232–1256, 2017.

[99] H. Kharrufa, H. Al-Kashoash, Y. Al-Nidawi, M. Q. Mosquera, and A. H. Kemp, "Dynamic RPL for multi-hop routing in IoT applications," in *Proceedings of the 13th Annual Conference on Wireless On-Demand Network Systems and Services (WONS '17)*, pp. 100–103, February 2017.

[100] A. Aijaz and A. H. Aghvami, "Cognitive machine-to-machine communications for internet-of-things: a protocol stack perspective," *IEEE Internet of Things Journal*, vol. 2, no. 2, pp. 103–112, 2015.

[101] S. Basagni, C. Petrioli, R. Petroccia, and D. Spaccini, "CARP: a channel-aware routing protocol for underwater acoustic wireless networks," *Ad Hoc Networks*, vol. 34, no. supplement C, pp. 92–104, 2015, Advances in Underwater Communications and Networks.

[102] Z. Zhou, B. Yao, R. Xing, L. Shu, and S. Bu, "E-CARP: an energy efficient routing protocol for UWSNs in the internet of underwater things," *IEEE Sensors Journal*, vol. 16, no. 11, pp. 4072–4082, 2015.

[103] B. L. R. Stojkoska and K. V. Trivodaliev, "A review of Internet of Things for smart home: Challenges and solutions," *Journal of Cleaner Production*, vol. 140, pp. 1454–1464, 2017.

[104] C. Dobre and F. Xhafa, "Intelligent services for big data science," *Future Generation Computer Systems*, vol. 37, no. supplement C, pp. 267–281, 2014, special Section: Innovative Methods and Algorithms for Advanced Data-Intensive Computing Special Section: Semantics, Intelligent processing and services for big data Special Section: Advances in Data-Intensive Modelling and Simulation Special Section: Hybrid Intelligence for Growing Internet and its Applications.

[105] C. Liu, C. Yang, X. Zhang, and J. Chen, "External integrity verification for outsourced big data in cloud and IoT: a big picture," *Future Generation Computer Systems*, vol. 49, no. supplement C, pp. 58–67, 2015.