

Review

Networking Architectures and Protocols for IoT Applications in Smart Cities: Recent Developments and Perspectives

Dimitris Kanellopoulos ^{1,*}, Varun Kumar Sharma ², Theodor Panagiotakopoulos ^{3,4,*} and Achilles Kameas ³¹ Department of Mathematics, University of Patras, 26500 Patras, Greece² Department of Computer Science and Engineering, The LNM Institute of Information Technology, Jaipur 302031, India; varunksharma.102119.cse@gmail.com³ School of Science and Technology, Hellenic Open University, 26335 Patras, Greece; kameas@eap.gr⁴ School of Business, University of Nicosia, 2417 Nicosia, Cyprus

* Correspondence: d_kan2006@yahoo.gr (D.K.); panagiotakopoulos@eap.gr (T.P.)

Abstract: Numerous municipalities employ the smart city model in large cities to improve the quality of life of their residents, utilize local resources efficiently, and save operating expenses. This model incorporates many heterogeneous technologies such as Cyber-Physical Systems (CPS), Wireless Sensor Networks (WSNs), and Cloud Computing (ClCom). However, effective networking and communication protocols are required to provide the essential harmonization and control of the many system mechanisms to achieve these crucial goals. The networking requirements and characteristics of smart city applications (SCAs) are identified in this study, as well as the networking protocols that can be utilized to serve the diverse data traffic flows that are required between the dissimilar mechanisms. Additionally, we show examples of the networking designs of a few smart city systems, such as smart transport, smart building, smart home, smart grid, smart water, pipeline monitoring, and control systems.



Citation: Kanellopoulos, D.; Sharma, V.K.; Panagiotakopoulos, T.; Kameas, A. Networking Architectures and Protocols for IoT Applications in Smart Cities: Recent Developments and Perspectives. *Electronics* **2023**, *12*, 2490. <https://doi.org/10.3390/electronics12112490>

Academic Editors: Marek Pagač, Chuan Pham, Van Dung Nguyen, Huynh Kha Tu, Huu Khoa Tran and Tran Anh Khoa

Received: 28 April 2023

Revised: 28 May 2023

Accepted: 29 May 2023

Published: 31 May 2023



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

1. Introduction

Nowadays, several municipalities implement the smart city model [1] to improve the quality of life for their citizens and the efficient use of city resources. Intelligent services can decrease operational costs and resource expenditure in smart cities. They can enhance performance and operations in a wide variety of smart city applications (SCAs) including transportation, healthcare, energy, education, and many more. Smart services are provided by various cutting-edge technologies supporting the smart city model. Examples of these technologies include the internet of things (IoT), Wireless Sensor Networks (WSNs), Cyber-Physical Systems (CPS), Cloud Computing (ClCom), fog computing (FoC), big data analytics, and robots.

IoT is the core technology used in smart cities, bringing plentiful human life benefits [2]. IoT enables the integration of physical objects/smart things into urban environments where innovative services are offered to support every activity at any time and from any location [2]. Things are monitored by IoT applications that make direct decisions for their efficient management. Moreover, things state their conditions, such as battery status and fault reporting for prognostic maintenance. WSNs offer real-time monitoring of the state of the infrastructure and resources in a smart city [3]. Wireless sensor devices can also obtain physical environment information such as temperature. In a CPS, the computation, networking, and physical processes are put together to control and monitor the physical environment of a smart city [4]. In smart cities, CPSs are employed to offer practical connections between the virtual and physical worlds. Applications for smart cities can be sustained by the ClCom paradigm that provides a scalable and affordable platform

for computation and IoT data storage [5]. FogC offers reduced latency, greater mobility, location awareness, streaming, and real-time response for SCAs [6]. Smart cities have dispersed vast numbers of sensors, and thus large-scale data processing requires a complex infrastructure. Robotics in the cloud can be an effective computing tool for IoT applications that require a lot of data processing [7]. To improve the services offered by smart cities, big data analytics is employed to generate intelligent and optimal temporary and lasting decisions [8].

The abovementioned technologies are used to implement numerous smart city services [9,10]. For instance, intelligent transportation services are applied to improve route planning and avoid jamming in city streets. These services can enhance vehicular safety and make possible self-driving cars. Furthermore, parking services and smart traffic light controls are provided. Smart energy services [10] (e.g., intelligent energy management and energy consumption prediction) are used to sustain smart grids and smart buildings. These services can also offer improved utilization of renewable energy. Additional smart services are engaged in real-time monitoring of bridges, tunnels, water networks, train and subway rails, and gas and oil pipelines. Structural health monitoring is also feasible using smart services [11]. Last but not least, there are smart services that focus on monitoring the environment, public safety, and security of citizens [12].

All these smart city services necessitate a reliable networking infrastructure to efficiently exchange messages between the modules of a smart city system implementing a particular smart service. In particular, smart city services need a variety of networking and communication technologies for their completion because they are proposed for dissimilar scales. For example, smart services for smart buildings must be implemented based on Zigbee (IEEE 802.15.4) or Bluetooth (IEEE 802.15.1) network protocols. On the other hand, smart services for the smart grid must be mainly implemented using the WiMAX (IEEE 802.16) network protocol. From another viewpoint, smart city services can exploit dissimilar network and communication models and solutions.

Until now, the networking and communication components of smart city systems have received little research attention. To the best of our knowledge, a comprehensive survey of network architectures and protocols for IoT applications in smart cities does not exist and is the goal of this study. The communication and networking issues involved in smart city systems are examined in this study. This paper considers networking technologies, topologies, and communication requirements for such systems. It also examines if current network protocols are appropriate for certain smart city services. This paper surveys recent developments in networking architectures to support SCAs. As this is an active area, this paper is important to support new research in this field. The paper contributes as follows:

1. It presents network requirements of the major SCAs including intelligent transportation, smart buildings, pipeline monitoring and control, smart water networks, smart grids, and manufacturing control and monitoring.
2. It reviews networking architectures used for the above applications focusing mainly on the protocols' suitability.

The remainder of this paper is structured as follows: Section 2 describes SCAs; Section 3 presents network requirements and protocols used for important SCAs; Sections 4 and 5 analyze protocols and network architectures for smart grids, smart buildings, smart water and pipeline network monitoring, and smart transportation; Section 6 summarizes the paper, while Section 7 provides open research directions; lastly, Section 8 concludes the paper. Figure 1 provides the layout of the survey.

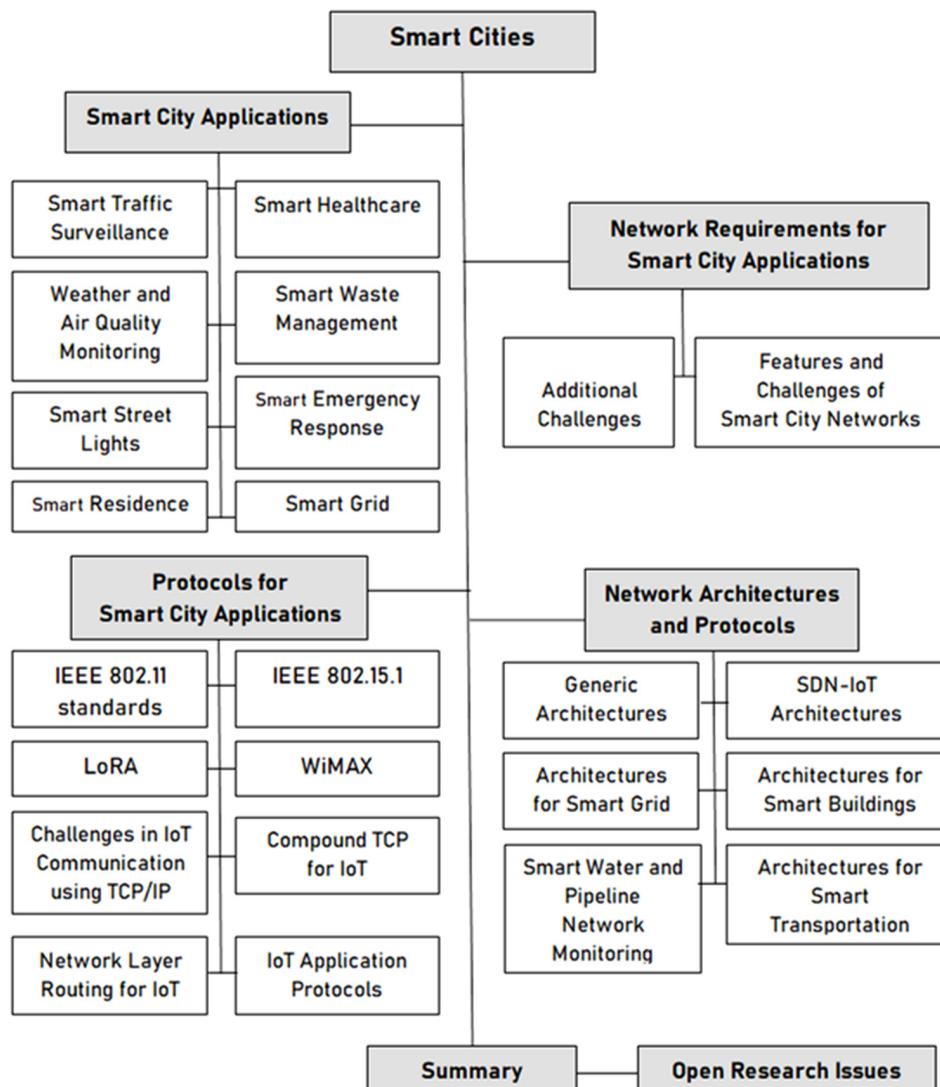


Figure 1. The layout of the survey paper.

Systematic Literature Review

Article Selection Method: We provide a Systematic Literature Review (SLR) methodology [13] with particular notice to studies related to networking architectures or protocols for IoT applications in smart cities. The SLR was employed to systematically study networking architectures and protocols for IoT applications in smart cities. We proposed a research question to cope with the key issues of networking architectures and protocols for IoT applications in smart cities.

Question Formalization: Key issues and challenges in the field were identified. Such issues were network architectures for IoT, network protocols for IoT, IoT applications for smart cities, and smart city applications. This study answers the next research question:

RQ: What is the emphasis of networking architectures or protocols for IoT applications in smart cities?

This question determines the number of studies focusing on network architectures and protocols for IoT applications for smart cities that have been published to date to emphasize its significance in smart cities.

Article Selection Process: The article selection process is performed in three stages:

1. Automated keyword-based search;
2. Selection of the article based on the title, abstract, and quality of the publication;
3. Elimination of inappropriate articles.

In the first stage, the search process is automatically performed using searching on popular academic databases such as IEEE explorer, ACM, Wiley, Springer, Science Direct, SAGE, and Google Scholar. The following search string was defined by adding other spellings of the main elements to find relevant articles. The search string was as follows:

("IoT" OR "Internet of Things") AND ("network architecture" OR "network protocol" AND "smart cities" OR "smart rural" OR "smart village" OR "smart traffic" OR "smart transportation" OR "smart street lights" OR "smart energy" OR "smart grid" OR "smart buildings" OR "smart home" OR "smart residence" OR "home automation" OR "smart water" or "smart waste management" OR "smart healthcare" OR "smart rural" AND "Cloud Computing" OR "edge computing" OR "software-defined networking" OR "Artificial Intelligence").

We found 264 articles from journals, conference proceedings, books, and patents. These articles were published between 2013 and 2023. In the article selection based on the quality of the publisher stage, the search string was constrained by searching for conference papers and journal articles of IEEE, ACM, Sage, Wiley, Science Direct, and Springer, in order to guarantee that only high-quality publications and articles were selected for the review. Consequently, 240 articles were selected.

In the third stage of eliminating the inappropriate articles, a Quality Assessment Checklist (QAC) based on [13] was developed, wherein those articles emerging from the initial search were refined. After reading the abstracts, we eliminated the unrelated articles. The entire body of the remaining papers was checked, and those which were not related to our concerned field were also crossed out. After eliminating inappropriate articles, only 226 studies were identified.

2. Smart City Applications

This section discusses the main SCAs used in diverse domains. To understand what type of assistance is needed by the networking infrastructures offered for SCAs, their advantages and design problems were addressed.

In the energy sector, SCAs are being used to increase the reliability, efficiency, and sustainability of electric energy generation and distribution in smart grids [14]. A smart grid is a new power grid system that automatically collects and reacts to available information about supplier and consumer behavior. Smart grids use CPS to supply self-monitoring and superior control mechanisms for power generation and consumer demand, improving grid reliability and efficiency. CPS systems are also used to manage the process of producing renewable energy from wind turbines [15].

Certain applications are utilized in smart buildings to monitor and manage energy consumption [16]. CPS controls the equipment in the buildings, including the Heating, Ventilation, and Air-Conditioning (HVAC) systems; appliances; and lighting systems. Different kinds of sensor nodes, which keep track of the current state of the environment and energy consumption, are typically included in smart building systems. A centralized monitoring and control system receives observations and measurements from these sensors. Based on reported observations, current operational circumstances, and environmental factors, the control system employs intelligent algorithms to manage the sub-systems employed in the buildings to optimize energy consumption.

Intelligent transportation is another SCA that has attracted a lot of interest in the transportation sector. Applications related to vehicle safety are among the most crucial types of such applications. Vehicles can be equipped with a variety of safety features, such as blind spot monitoring, emergency braking, collision avoidance systems, and lane change warning signs. To improve driving safety, these applications offer full or semi-automatic operations. Real-time and reliability support in detection and response are these applications' most crucial characteristics. Applications for enhancing vehicle safety must be dependable and able to operate in real-time in all aspects such as threat observations, decision making, communication, and actions. However, the software cannot handle high levels of incorporation across all the relevant devices and guarantee real-time and

trustworthy replies. Furthermore, self-driving vehicles are regarded as crucial SCAs [17]. They combine all the aforementioned capabilities with vision and monitoring equipment to provide the vehicle the ability to traverse the roads using sensed data and intelligent software that evaluates and reacts to these data in real-time. Intelligent traffic light controls, which incorporate device monitoring across numerous locations to precisely forecast traffic patterns, are another application of intelligent transportation. The authors of [18] present an example of intelligent traffic lights.

Water networks are maintained using smart city technology to increase their intelligence, efficiency, dependability, and sustainability. CPS systems are integrated into water networks to add smart characteristics to the processes of water distribution [19]. Offering early warning systems to identify problems in water networks is one of these duties. For instance, it is simple to identify leaks and pipe bursts. Quick, temporary fixes can be implemented to prevent water wastage and future network threats or damage [20].

WSN-based monitoring of greenhouses is another SCA. Such monitoring provides well-organized control for appropriate soil, climate, lighting, and water level in greenhouses [21]. Other smart city systems are deployed in the industry to automate, control, monitor, and improve manufacturing procedures [22,23]. Finally, smart-healthcare systems based on edge computing [24] are proposed to monitor and examine the physical health of users [25].

Figure 2 shows some important applications including smart traffic surveillance and management, smart healthcare, weather and air quality monitoring, smart waste management, smart street lighting, smart emergency response system, and smart home.

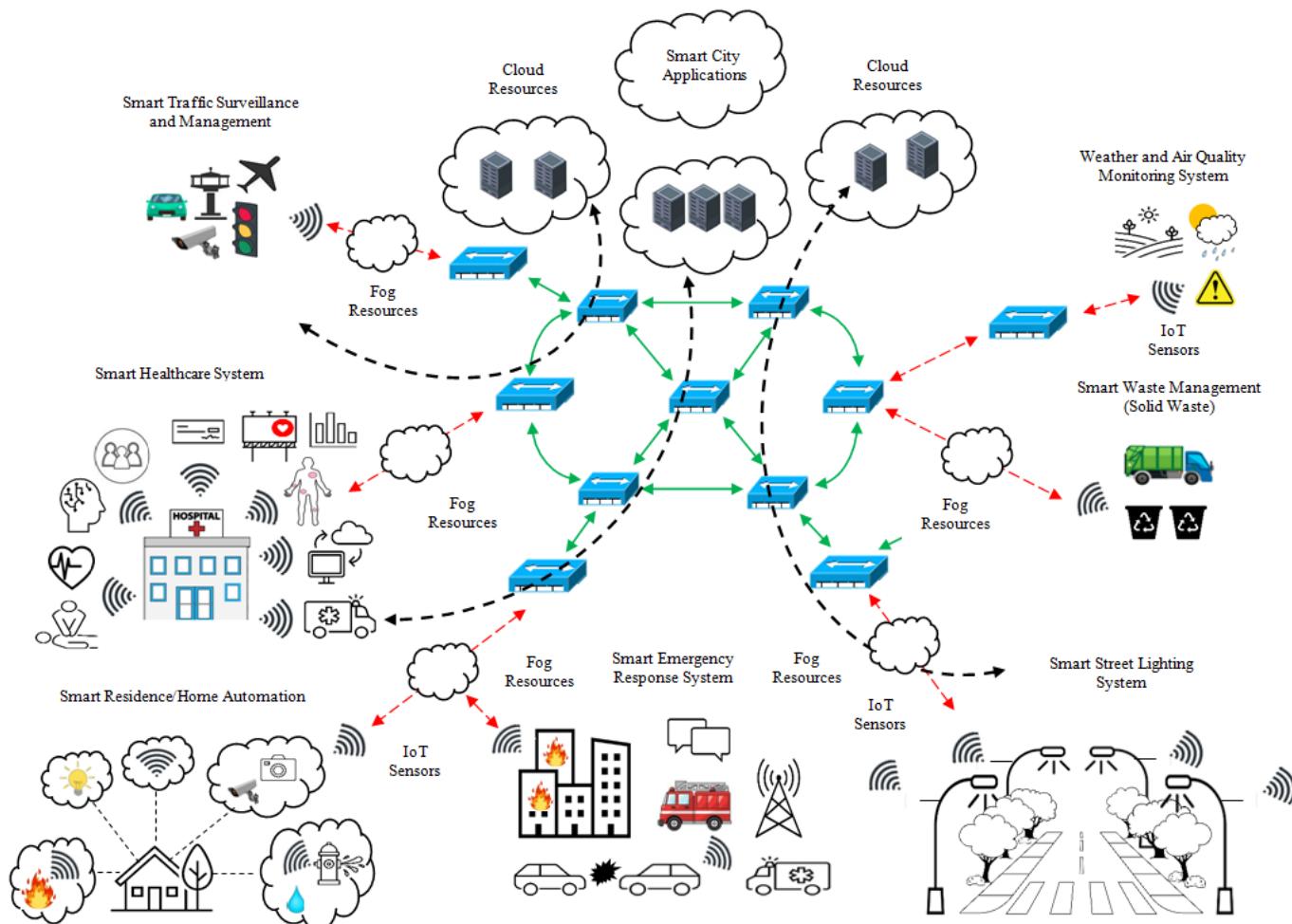


Figure 2. Facilitating networking and communication amongst SCAs.

Analysis of Smart City Applications/Systems

This subsection analyses the SCAs shown in Figure 2.

Smart Traffic Surveillance Systems: These systems are based on centralized processes and may fail due to networking problems. Thus, to automate such an innovative system, centralized and distributed methods must be used to maintain local servers. Javaid et al. [26] suggested a smart traffic management system using a mixture of centralized and decentralized processes to optimize the flow of vehicles on roads and an algorithm to manage a variety of traffic conditions efficiently. In the context of smart cities, effective traffic management implies that a decision-making model identifies and quantifies traffic congestion as well as predicts traffic patterns. Afrin and Yodo [27] offered a theoretical analysis that takes into account such effective traffic management. Notably, existing decision-making models are primarily devoted to urban and highway traffic management, not considering the closed campuses and collector roads scenarios. Sarrab et al. [28] identified this weakness and proposed an IoT-based system model that collects, processes, and stores real-time traffic data for such an unusual scenario. In an IoT-based traffic management system, various challenges emerge. These challenges include security issues, extremely sophisticated networking equipment, network overhead, required adjustments, and specific information fields in the protocol header and structure, as well as higher costs.

Smart Healthcare Systems: For real-time monitoring of health parameters, these systems are progressively being associated with and connected via the Internet to numerous types of available smart wearable sensing and computing devices. These systems face several problems [29] that must be resolved. A security/privacy perspective, inter-realm authentication, interoperability issues, device-to-device informal communication, and collection and management of medical data are among the issues on this list. Alromaihi et al. [30] addressed issues related to cyber-security while using IoT for such applications. They sought to examine secure techniques' deployment and implementation from the perspective of preventing and reducing cyber-attacks on IoT devices. Some crucial surveys and reviews [31,32] on smart healthcare applications tackle the problem of integrating IoT systems with any healthcare application particularly.

Weather and Air Quality Monitoring Systems: These systems use environmental monitoring stations, which are extremely pricey to acquire and maintain. For example, these stations require engineers with specialized skill sets and data analysts. Therefore, it is impractical to deploy such monitoring stations densely. Instead, they are often deployed sparsely, which creates the problem of limited spatial resolutions for useful measurements. Lately, cheap monitoring sensors have evolved in the market, significantly assisting in refining the granularity of monitoring [33]. Highlighting the same problem, the authors [33] emphasized the drawbacks of these inexpensive sensors (particularly with air quality monitoring sensors). For instance, these sensors frequently struggle with the issue of cross-contaminations in the presence of multiple ambient pollutants. Moreover, these sensors are extremely susceptible to unexpected variations in humidity, temperature, and wind direction, and as a result, their accuracy deteriorates with time. A recalibration routine might be a way to maintain and enhance such accuracy. However, because it would take a lot more time and work, this technique is highly improbable and would not work for large-scale deployments. In a weather monitoring system, the monitoring is highly complex and involves three steps [34]:

- (1) *Observing:* It can be performed by monitoring satellite imagery, precipitation reports, surface data, and gathering data from other nearby forecasters.
- (2) *Forecasting:* It can be performed by forecasters as short-term and long-term forecasting. Short-term forecasting is carried out by evaluating the current weather conditions and projecting them over the next few hours using knowledge of the mechanics of the weather. Long-term forecasting, however, is possible through weather (numerical) modeling and the projection of such modeling using computer simulations. To produce these simulations for future forecasting, these modeling techniques use environmental data from satellite photography, weather balloons, and surface ob-

servations. Following completion of the forecasting, the forecasters translate the produced simulated expected output into a perceptible format for non-specialists so that they can respond appropriately.

- (3) *Communicating:* Finally, they communicate such output or forecasted information to appropriate authorities.

Despite the fact that all of these computer models are used to forecast the weather, the success of each one is largely influenced by three different elements: (a) the quantity of precise data; (b) the length of time needed to analyze that data; and (c) the complexity of dynamic atmospheric weather events. A large part of collecting accurate data for a region is the placement of weather stations. They may occasionally be stationed distant from rural areas in a city area. Because of this, they are unable to gather enough information for desert, sea, or even rural areas to supply the computer models used to predict weather conditions accurately. Forecasters also use satellite data to combat this issue. However, because of cloud cover and significant changes in the amount of water vapor in the atmosphere, satellite data accuracy can occasionally be unreliable. Moreover, the topographic image and map information or surface/land features change substantially in a shorter area. Hence, it further impacts temperature and precipitation values significantly. This further makes things harder for a computer model to predict accurately. Hence, there is a need to re-evaluate and re-modify such models' mathematical equations so that they can predict the changes more accurately.

Smart Waste Management Systems: Automated smart waste management is crucial for the following reasons: (1) due to a lack of waste disposal infrastructure; (2) thin or delicate waste collection methods being required; (3) lack of effective waste logistics management; (4) insufficient use of cutting-edge trash treatment and recycling technologies; and (5) lack of workers and specialists with the necessary technical and non-technical skills to handle garbage disposal and the associated infrastructures. Smart waste management schemes include various steps such as (1) waste collection; (2) differentiation of waste as per their biological and physical properties; (3) storage; (4) transportation of waste into garbage disposal infrastructures/treatment plants; and (5) waste treatment and disposal. Sosunova and Porras [35] identified issues and challenges while collecting and analyzing data from smart deployed sensors on garbage bins. Their study investigated some operational issues such as the management of waste vehicles and urban infrastructure and smartly managing waste vehicle routes.

Smart Street Lighting Systems: This system is a network-oriented solution that uses streetlights fitted with specific actuators and sensors, implying a wide range of facilities and connectivity interfaces [36]. The street lighting application (described in [37]) has a mechanism that gathers or monitors environmental data and then evaluates street lighting with the use of smart wireless nodes (fitted out with numerous forms of sensors and actuators). These smart nodes are mounted atop the towers that hold the streetlights, and they are connected to the Internet by way of a gateway device. Zanella et al. [37] insist that their system could assist in gathering environmental parameters such as humidity, air temperature, and CO level. Moreover, the authors stated that optimizing street lighting efficiency is a paramount concern that must be addressed. This monitoring system makes it possible to maximize efficiency since it allows for the adjustment of streetlamp intensity in response to the time of day, the presence of people, and the weather. Although this system is simple and built on the IoT concept, it will inevitably contain crucial concerns that require particular attention, such as complicated networking solutions and communication among heterogeneous devices. However, selecting the right light lamp is critical for a power-efficient lighting mechanism. Their selection is based on how effective they are in terms of power usage and lifespan. The existing metropolitan system relies on Metal Halide (MH) or High-Pressure Sodium (HPS) bulbs. Unlike LEDs, these bulbs are frequently seen as being inefficient in terms of power consumption and requiring significant maintenance, which adds significantly to the cost. In addition, the system should be designed following the advised design standards (it must adhere to the current standard CEN/TR 13201) [36].

Currently, there are three kinds of control systems for smart lighting systems in use: centralized, decentralized, and hybrid. Nevertheless, these systems are susceptible to a variety of security assaults. Moreover, not much effort has been made into this problem thus far.

Smart Emergency Response Systems: Such a system ensures the safety and security of its residents. It can be utilized for crime detection and prevention, dealing with natural calamities and accidents, and law enforcement [38]. Data collection is first and foremost important for the designing portion of these applications. Depending on the gathered facts, the development of intelligence (which aids in making important decisions) and the ability to respond swiftly and quickly are the issues that require special attention. When it comes to gathering data, we can make use of CCTV cameras and sophisticated traffic sensors. A developer can create and put into action a crucial learning scheme that will conduct predictive analysis and gather intelligence on top of the data gathered. Therefore, this kind of predictive analysis has the potential to gather significant information that will help the relevant authorities (e.g., the fire safety department, the police department, and law enforcement agencies) take the proper security and preventive measures. The concept of widespread surveillance has important benefits for security and safety. However, keeping track of such vast amounts of data also prompts a lot of worries and issues for designers and developers, including storage; the effectiveness of learning algorithms; and, most importantly, the question of whether it is morally right or acceptable to keep track of each individual (a privacy issue). In addition, a very important point is whether this kind of widespread surveillance is feasible, especially for nations such as China and India, where a city's population can exceed that of a whole nation. Further, Gharaibeh et al. [38] claimed that combining information transmission technologies with well-implemented data analytics models is necessary for quick and swift collaboration. To save as many lives as possible during natural disasters, it is imperative to gather, assess, and communicate vital information to the relevant authorities. As a result, there is currently a lot of work being done to enhance the performance of information exchange systems. Although this system is based on the IoT concept and is relatively simple, it faces important problems that need consideration, such as complex networking solutions and information sharing across heterogeneous devices on time (time-sensitive application).

Smart Residence/Home Automation: A smart home has highly developed systems such as a control system for devices or objects (such as fans, lights, music systems, TVs, and other smart appliances), automated door openers, smart appliances that may send users remote status updates, smart refrigerators, and washing machines. A user can control the majority of smart home appliances remotely with two recently produced gadgets: *Google Home* and *Amazon Echo*. In a smart home, the end-user demands a high-speed internet connection, so they can access networking sites that control the home with HD live streaming services. In contrast, a smart healthcare application needs safe connections to computing servers in the cloud for managing sensitive private information. Hence, data management systems must address a crucial issue, namely, the necessity to concentrate on data distribution based on various end-user categories rather than just recommending distinct data distribution among various end-user groups [38]. The concept of smart home automation raises serious concerns about security and privacy risks. A smart home includes security monitoring systems with motion sensors, wirelessly opening smart door locks, televisions, phones, and other smart appliances that are highly outfitted with cameras and microphones. Although these gadgets improve the system, little research has been done on their privacy and security features. If we conduct a thorough analysis of these gadgets, we will discover that their manufacturers offer either very few or no security features at all. Indeed, Fernandes et al. [39] provided their eye-opening views after carefully examining Samsung's SmartThings framework (programming) and their SmartApps market. They argued that more than 50%—exactly 55%—of these smart applications are already more privileged by default and as a result, do not need to access unrelated applications. As a result, hackers can use them with ease. Apart from this, according to a published document

by WikiLeaks [40], the Central Intelligence Agency (CIA) has all the tools to access, control, and hack these smart home applications anywhere in the world. Furthermore, criminal entities and hackers could seize control of smart personal devices, capture delicate private information, and exploit that information immorally typically through user tracking and profiling. Additionally, a hacker may break into one of these smart applications, grab vital information, and then use it to launch any kind of attack. For instance, based on motion sensors, security camera feeds, and power usage patterns, a burglar can determine where and when to break into the house. By locating the authentication credentials of authorized parties, they can compromise smart door locks [41]. Better security-aware hardware and software (as well as the related common standards) must be developed to safeguard against all these attempts so that high-tech appliances, sensors, actuators, etc., are impervious to such security and privacy attacks.

Smart Grid Networks: The functionality of the traditional electricity grid is unidirectional (i.e., electricity is transmitted from electricity-producing sources to end-customers). Electricity has been moving from power plants to users in a single direction thanks to the deployment of electricity grids. The existing grid system operates in an open-loop fashion since there are not any adequate communication infrastructures in the distribution sector. Moreover, the main distribution center has little or no real-time knowledge of the system's operating conditions and dynamically changing load. There are also several technical, economic, and environmental problems with this conventional approach. Therefore, this conventional system must become dependable, manageable, and scalable, as well as flexible, secure, and interoperable [42].

The smart grid is the next invention of the Electric Power System (EPS) that incorporates quicker, more secure, and reliable communication networks [43]. Smart grids supplement the conventional electricity grid by incorporating renewable energy sources such as biomass, solar energy, and wind energy. These energy sources are much cleaner and more ecologically friendly than non-renewable energy sources such as fossil fuels. However, it is important to identify the most suitable communication technology for the smart grid's successful implementation and deployment. The smart grid's overall communication style is unique compared with conventional network communication patterns. The communication network architecture of the smart grid must be able to handle information exchange between sensors, actuators, smart electronic devices, and numerous smart meters in such a particular environment with little to no human intervention. This type of communication, called Device-to-Device (D2D) communication, is autonomous and may be initiated in response to an event or at regular intervals. Notably, depending on how these smart grid applications were built, their QoS requirements and characteristics differ greatly in terms of delay, burst size, and packet arrival rate. For example, the latency requirement of a smart meter event and a substation event are quite different [44]. In intelligent grid networks, the monitoring, managing, and controlling functions inside the same network present the issues of flexible QoS differentiation. Moreover, applications based on the smart grid can be developed and implemented using the current wireless and wired networking infrastructure and technologies. For some devices, such as smart meters, designing and standardizing acceptable smart grid-based protocols is a critical matter [45]. Furthermore, these smart grid-based networks are too dependent on intelligent sensors, actuators, and other devices. This makes them extremely vulnerable to attacks by malicious users. These smart grids could be taken over by malevolent users or hackers, who could then obtain unauthorized access to many smart meters and alter crucial data. Moreover, as the existing electricity system is insufficient for establishing smart grid systems, high-level adjustments to current power infrastructure scenarios are required. Subsequently, these smart systems require high installation costs because the installation requires a large number of smart meters, sensors, and actuators for sensing and data collection [46]. The efficient operation of such a smart grid system also necessitates a dependable, consistent, and error-free network channel. Therefore, it will be challenging for developers of such intelligent applications.

Many surveys [42–45,47] reviewed communication frameworks for smart grids, smart-grid-based networking technologies, traffic management, and the requirements of numerous smart grid applications. Further, Kansal and Bose [48] presented their insights on transmission grid applications regarding their latency and bandwidth requirements.

3. Network Requirements for SCAs

This section considers several communication requirements including reliability, delay tolerance, bandwidth, power consumption, security, network type, heterogeneous network support, and mobility support. It also studies the aptness of different network protocols for dissimilar SCAs.

Smart city services and applications need robust and dependable communication support as well as an effective networking infrastructure, which will permit competent message-sharing procedures among the components of the smart city systems [49]. Every smart city system has an intricate networking architecture made up of various networking components. Therefore, smart city systems are innately required to have a variety of networking requirements. To access the far-off destination, which may be clouds, the network traffic from a broad variety of deployed diverse applications uses a common networking architecture and resources. These resources may consist of switches, routers, communication connections (links), and other forms of network middle-boxes. The idea of accessing faraway clouds or far-off destinations or remotely distributed apps consequently brings up problems with high packet loss probability, significant delay, and constrained network bandwidth. In addition, security is a serious issue that must be considered when developing, implementing, and deploying intelligent applications for smart cities. Otherwise, users would be reluctant to approve the use of such applications in the absence of adequate security safeguards. Such intelligent applications need a high-speed networking environment where the quick reaction may be managed with the support of the ability of a fast-processing speed. Furthermore, a variety of apps can be implemented in the context of a smart city, based on their usefulness and relevance to the users. These applications, however, have different networking requirements, particularly in terms of response and security [50]. For example, the networking requirements of smart emergency response systems are quite different compared to other applications such as smart healthcare systems. Emergency response smart systems must be exceedingly secure and quick to react [50]. In contrast, smart-healthcare-based systems or apps do not necessarily need to be especially dynamic.

- **Network Protocols:** Monitoring applications for smart cities often use a dense network of heterogeneous sensor nodes, including fixed sensor nodes, mobile sensor nodes, and crowd sensing nodes. Long-Term Evolution (LTE) [51], LTE for Machines (LTE-M), extended coverage GSM IoT, and fifth-generation (5G) technologies [52] are intriguing options to support such heterogeneous networks. First, the bulk of crowd-sensing nodes (smartphones) is already supported by LTE communications. Consequently, no further wireless communication devices are required. To save energy, LTE and 5G can be utilized on the sink nodes (also known as cluster heads) to allow the data gathered by the sink nodes to be transmitted to the monitoring center via base stations (the backbone network), as opposed to multihop relaying.
- Zigbee [53], WiFi, and Bluetooth can still be used for the traditional stationary nodes to communicate within clusters. This layout has the advantage of allowing the sensor node clusters to be separated from one another while maintaining network connectivity. Additionally, the moderate number of nodes in each cluster makes maintenance simpler. In addition to supporting larger networks, LTE and 5G technologies also make possible sensor nodes with faster data rates, improving the performance of real-time monitoring [54]. Applications for crowd sensing, for instance, can accommodate video streams taken by cameras on smartphones or moving vehicles. The fast data rates provided by LTE and 5G can potentially be advantageous for the sink nodes or clusters. The use of vibration data (accelerometer readings) in structural health monitoring applications of bridges, tunnels, or towers is fairly common. The cluster heads will be

able to send the vibration data in this situation in real time. In conclusion, practically all applications for smart city monitoring that demand a high data throughput and minimal delay may be satisfied by LTE and 5G. Additionally, there are some new sensor node standards, such as IEEE 802.11ah [55], LoRaWAN [56], and Narrowband-IoT (NB-IoT) [57]. These narrowband protocols offer numerous advantages: greater coverage, improved scalability, reduced energy usage, and increased device longevity. Researchers have tested these standards in more than a few applications, including street lighting, energy metering, and home automation, even though some are still being discussed and revised. The new narrowband communication standards enable the sensor nodes to run more sustainably, which is beneficial for applications that aim for long-term monitoring. In addition to these protocols and standards, the FogC architecture [58] aids in monitoring smart cities. In such an architecture, the mobile users (the potential crowd-sensing providers) and the cloud are connected via fog servers. These fog servers are WiFi access points or cellular base stations. Mobile users are more inclined to participate in sensing since they may upload their crowd-sensing measurements to the fog server in just one hop, significantly decreasing the cost and energy usage compared to cellular networks. As a result, such an architecture can give us better sensing coverage. Using the measurements from the mobile users and the WSNs, the fog servers can perform some basic regional estimation based on the FogC architecture, such as the nearby traffic conditions. The service latency and response time are then decreased because mobile users can access such estimates directly from the fog servers rather than from a remote cloud through a backbone network. Lastly, using the appropriate networking protocols for each SCA is crucial to getting the best possible trade-off between delay, energy use, and cost. The networks may be hierarchical so that diverse roles and functions can be assigned at various layers to increase the networks' dependability and cost-effectiveness. As a result, certain nodes may be able to transmit data utilizing various protocols.

- **Bandwidth requirements:** Many video applications in smart cities require high bandwidth [59]. In these applications, sensors capture video from the physical environment. Moreover, video transmission is more bandwidth-hungry than the conventional scalar data traffic in IoT. Examples of these applications are intelligent multimedia surveillance systems for home monitoring, multimedia-based industrial monitoring systems, traffic monitoring systems for road safety, and remote multimedia-based monitoring of an environmental system.
- **Delay Tolerance:** Some SCAs, such as smart transportation, only tolerate a small amount of end-to-end delay. For example, to prevent imminent danger to the vehicle or potentially fatal crashes, the data that are being relayed must arrive within microseconds. Therefore, the control systems must react in time. However, other applications have a higher tolerance for delays [49]. Such applications rely on data monitoring and information gathering for upcoming analysis.
- **Power Consumption:** Another crucial need for applications is power consumption. Smart grid systems and other applications with local high-energy sources can tolerate protocols with higher energy expenditure levels [45]. Other applications have medium power needs and require energy sources with limited capacities. One example of such an application is intelligent transportation. Other applications demand protocols with low or very low energy consumption characteristics since they have limited energy resources. Unmanned aerial vehicles (UAVs), smart water networks, and pipeline monitoring for gas and oil are a few examples of such uses.
- **Reliability:** The majority of applications have medium reliability requirements. A typical example of such applications is smart water networks. Some other applications have high-reliability necessities such as intelligent transportation and smart grids [49].
- **Security:** The majority of applications need medium to high security. Applications such as production control and monitoring, for instance, need medium security, whilst

others, such as smart grids, need high security because of the sensitivity of the data and the importance of the operations carried out [50].

- **Heterogeneity of network protocols:** The majority of smart city systems use networking protocols that link the system's parts together. Intelligent transportation and smart buildings are two examples of such systems. These protocols must coexist in such situations without conflicting with one another. To ensure seamless and effective operation, it is also necessary to correctly map the control information in the headers at the various networking stack tiers used by the many heterogeneous protocols and networks.
- **Wired/wireless connectivity:** The majority of SCAs that include wireless connectivity are UAVs and monitoring of gas and oil pipelines. Others, including intelligent transportation and smart buildings, use wired and wireless connectivity [50]. In these situations, wired networking may be used for communication within a specific physical system (such as within a UAV), while wireless communication may be used to link the physical system to other such systems that are comparable to it or to the backbone and infrastructure networks.
- **Mobility:** Some systems, such as the smart grid, pipeline monitoring for gas and oil, and smart water networks, have low to medium mobility [50]. Other systems, such as UAVs and intelligent transportation, are quite mobile. Medium- to high-mobility smart city systems can be connected if the networking protocols are reliable and adaptable to node mobility without using up a large amount of bandwidth on control messages and related processing to react to changes in the network architecture.

Table 1 presents a qualitative comparison of the requirements of some SCAs. Each SCA has its own transmission range and is sustained by a heterogeneous network with low, medium, or high traffic rates and supporting high or low mobility of devices. Each SCA is based on different protocols and requires different bandwidth and latency tolerance. In each SCA, the number of devices involved differs.

Table 1. Networking aspects and qualitative comparison of SCA requirements.

Smart City Services/Applications	Seemingly Fitted Network Protocol/Technology/Standard	Transmission Range (Meters)	Bandwidth Requirement (Minimum)	Latency Tolerance	Number of Devices	Network	Mobility Support	Traffic Rate
Smart Traffic Surveillance	Cellular, IEEE 802.11, IEEE 802.16, IEEE 802.15.4	≈1000	M	M	≈1000	Heterogeneous	H	L
Smart Healthcare System	Cellular, IEEE 802.11, IEEE 802.16, IEEE 802.15.4, IEEE 802.15.6, IEEE 802.15.4j	≈1000	M	M	≈1000	Heterogeneous	L	L
Weather and Air Quality Monitoring System	Cellular, IEEE 802.11, IEEE 802.16, IEEE 802.15.4	≈1000	L/M	M	≈1000	Heterogeneous	L	L
Smart Waste Management	IEEE 802.11, IEEE 802.16, IEEE 802.15.4	≈100	L/M	H	≈1000	Heterogeneous	L	L
Smart Street Lighting System	IEEE 802.16 IEEE 802.15.4	≈10	M	H	≈100	Heterogeneous	L	L
Smart Emergency Response System	Cellular, IEEE 802.16, IEEE 802.15.4	≈1000	H	L	≈1000	Heterogeneous	H	H
Smart Residence/ Home Automation	IEEE 802.15.4, IEEE 802.15.1	≈100	M/H	L	≈10	Heterogeneous	L	M/H
Smart Grid Networks	Cellular, IEEE 802.16	≈100	L	M/H	≈100	Heterogeneous	L	M/H

IEEE 802.11: WiFi; IEEE 802.16: WiMAX; IEEE 802.15.1: Bluetooth; IEEE 802.15.4: Zigbee; IEEE 802.15.4j: Medical Body Area Network (M-BAN); IEEE 802.15.6: Body Area Network (BAN); Cellular: CDMA, GSM, UMTS; L: low; M: medium; H: high.

3.1. Additional Challenges

- **Interoperability:** Smart city systems are built on several heterogeneous networking protocols that use various media access control (MAC) mechanisms at the physical and data link layers. For the underlying technologies to be integrated seamlessly, these protocols must be interoperable [60]. In digital home networks, the IEEE 1905.1 protocol [61], which was created to offer a convergent interface between physical/data link layers and the network layer, is aimed to perform this function. Future research should focus on the creation of similar protocols to increase the support system for smart city systems.
- **Scalability:** A smart city platform must manage many devices that are connected to the city's infrastructure. Large amounts of city-related data, which are continuously produced and consumed by devices and client applications, must be stored and processed. The platform must simultaneously be able to handle hundreds of requests from users and services that rely on it. Thus, the scalability requirements change depending on the features of the city as well as the installed applications and services. Recently, Del Esponte et al. [62] suggested InterSCity, a microservices-based, open-source smart city platform that facilitates the collaborative development of large-scale systems, apps, and services for smart cities.
- **Load Balancing:** To maximize the usage of resources, load balancing assigns appropriate resources (i.e., network resources, storage capacity, computational resources, and energy resources) to user tasks. A large-scale IoT network performs better and avoids overload thanks to an effective load-balancing strategy [63]. Response time, cost, throughput, performance, and resource usage are all improved in terms of QoS parameters.
- **The Cloud/Edge/FogC Paradigms:** Cloud, Edge, and FogC facilitate the creation of smart city prototypes. These computing paradigms efficiently aid in the gathering, upkeep, and analysis of city data to pinpoint crucial city-related events that demand advanced processing and response [64]. Nonetheless, some IoT applications/systems for smart cities have strict processing and delay constraints. These real-time applications present the greatest obstacles to cloud-based services. Consequently, FogC and Edge Computing have emerged as viable computing paradigms for designing, implementing, deploying, and controlling such systems/applications. These paradigms bring computing resources closer to the IoT/device plane so that the primary computation can be done locally [65,66]. Each computing paradigm offers particular assistance based on the requirements of the application at hand. For example, to support a cloud-based SCA, ClCom offers centralized storage and processing capacity. For certain SCAs, ClCom can offer scalable processing power and data storage [5]. The features of ClCom (e.g., powerful processing, massive and scalable data storage, and cutting-edge software services) can be used to provide various support services for a variety of SCAs. ClCom can be the primary control and management platform for SCAs. The city's ClCom services can be used to connect various sensors and actuators for SCAs to gather, process, store, and manage sensor data for various SCAs. Vast volumes of data are gathered across a smart city, which can eventually become big data. The sophisticated platforms required for storing and analyzing this massive amount of data to improve operations and planning can be provided by Cloud Computing. To effectively support SCAs, the communication between city sensors and actuators and ClCom may involve various communication requirements. The network architectures used in the smart city should meet these requirements. Smart applications require the integration of sensors, actuators, and the cloud, and they can only function well with a robust network that offers good communication services linking both sides. The fact that cloud services are either provided at a single central location or across numerous distributed platforms in various locations is another problem that occurs when adopting ClCom for a smart city. For many cloud applications, the distributed ClCom strategy can offer greater quality and dependability support [67]. However,

it is frequently necessary to establish effective communication channels between the distributed CICom facilities that are present in various locations. The dependability and efficiency of the networks linking all components on both sides present another problem when using the cloud. There are issues with delays, dropped packets, and unstable connections when the Internet is involved. To consider these challenges, the SCA architecture must be carefully studied, as must the planning and control of network resources and communication models. However, some elements cannot be avoided, such as transmission delays. Ksentini et al. [68] investigated the QoS requirements of many IoT/cloud-enabled applications in a FogC environment to recognize QoS metrics. The authors introduced a QoS management model (QoS-Fog) that is inspired by the work of the OpenFog consortium on the reference architecture [69] for a FogC system.

3.2. Features and Challenges of Smart City Networks

A smart city network has the following features [70]:

1. *Large Densities*: A smart city network has a very large density as thousands of smart devices are distributed in the area of a city.
2. *Abnormal Traffic Patterns*: Cascading or synchronization among smart devices produces extremely bursty or correlated traffic patterns. These traffic patterns differ from the regular social-generated traffic patterns on which most existing schemes and technology used in our society are based.
3. *Disorganized Network Topology*: Unlike the widely used wireless connectivity features, smart city networks often adhere to a mesh network topology. The problem arises when smart devices communicate across unreliable wireless channels, where packet losses caused by wireless channel special properties are extremely common and eventually have an impact on the functioning of the smart city system. Therefore, it appears very improbable that a single high-throughput backbone can be deployable soon.
4. *Heterogeneity*: SCAs use a variety of technologies. In terms of power consumption, latency, throughput, and communication ranges, each of these technologies operates at a unique trade-off threshold. The involved dissimilar technologies must coexist on a single platform.
5. *Coexistence of heterogeneous technologies*: Communication technologies used in smart cities are distributed over the same radio space. At the same time, independent radio infrastructures are connected through a variety of wireless channels. Under such circumstances, the SCA must handle interference issues with competence.
6. *Security and Privacy*: SCAs are extremely vulnerable to several risks from malevolent users. The majority of specialized smart sensors, actuators, and other intelligent devices are developed by designers without considering security measures. Such applications may be highly vulnerable due to hostile actors' ease of access to these cutting-edge technologies and potential threats to people's security and privacy.

The main challenges for smart city networks are as follows [70]:

- *Lack of Standardization Solutions*: The IEEE 802.15.1 Bluetooth technologies for Personal Area Networks (PANs) and the IEEE 802.11 groups for wireless LANs adopt the concept of single-hop ad-hoc networking. These standards permit direct communication between two devices that are in the transmission range of each other. At the same time, the multi-hop ad-hoc networking paradigm enables the communication between any two devices which are not necessarily in their transmission range [71]. A problem that researchers must consider is how these intricate heterogeneous sets of devices (i.e., actuators, sensors, and other smart devices) can communicate uniformly without any standardization. Global distributors and manufacturers must propose and accept standardized network solutions that enable communication between diverse devices on homogeneous communication entities. The IEEE 802.15.4 standard is the dominant solution that presents a sophisticated version of the Physical Layer. This standard deals with the trade-off between data rate, communication range, and

power consumption. Several revisions or amendments (i.e., IEEE 802.15.4g and IEEE 802.15.4e) aimed at the SCA have just been released. The IEEE 802.15.4g amendment allows for a redesigned physical layer, allowing data rates and communication ranges compatible with neighborhood mesh (wide) networks. Then, it is followed by another cutting-edge modification, known as IEEE 802.15.4e, which modifies and enhances the method used by devices to access wireless channels while also using time-slotted channel hopping mode. This hopping mode further delivers low-power consumption and improved dependability. From another viewpoint, many researchers customized appropriate upper-layer protocols (i.e., the Internet Layer). They made the necessary modifications there to make smart applications compatible with conventional infrastructure. Since the network of low-power smart devices is confined, the researchers developed numerous adjustments to the Internet protocols to make them easily adaptable. For example, the most notable IETF projects are RPL [72] and 6LoWPAN [73], which greatly aid in creating and adapting smart city scenarios.

- *Interference problem:* Sophisticated technologies that are spread across the same radio space and independent radio infrastructures are linked via a range of wireless channels. Because of this, the smart application must handle interference problems in such situations. To share unlicensed bands, numerous networks must cooperate and be compatible with one another.
- *Vertical handover (soft):* Multiple radios are used by the rapidly expanding number of smart devices being developed. These devices should be able to recognize and use the best interface that is currently available while balancing power usage and throughput.
- *D2D Communications:* In the IoT context, there are numerous D2D communication demands. Unfortunately, conventional network gateways cannot handle such generated messages from heterogeneous devices.
- *Short Communicating Messages:* Internet-based protocols support and recommend acceptable performance for longer data packet scenarios. However, smart devices communicate with one another using short messages (since most of them are tiny and operate over low-powered battery devices). To this end, short communicating messages will positively impact network congestion detection and avoidance policies and promote in-band aggregation.
- *Local Network Traffic Pattern:* Smartphones and D2D-specific devices frequently use the same network infrastructure. However, most cellular data networks are exclusively planned, implemented, deployed, and managed for smartphone usage. Fitting traffic from these heterogeneous devices onto a single platform is now the main challenge that cellular data network providers face. It is difficult to integrate the traffic from these two types of heterogeneous devices into the same network infrastructure due to several intrinsic factors and the specified features of this traditional network. Additionally, D2D devices use a more significant proportion of scarce resources than smartphones, unnecessarily creating a problem of unfairness in the system [74]. Therefore, we must first comprehend D2D traffic patterns and how they differ from traffic patterns generated by smartphones. Understanding traffic patterns can provide insights into managing and allocating shared network resources more effectively and guarantee the highest level of service quality for both types of devices.
- *Security mechanisms:* Denial of Service (DoS) attacks are a remarkable threat to the security of smart city networks and must be identified. Some statistical methods have been proposed to solve this problem. Such a statistical method is presented in [75] that is based on feature distance maps that enhance the statistical analysis process. Another security mechanism is authentication, a process of identifying users and devices in a network and granting access to authorized persons and non-manipulated devices. Authentication is one method to mitigate attacks on the IoT systems such as the reply attack, the Man-in-the-Middle attack, the impersonation attack, and the Sybil attack [76]. To realize end-to-end security, the nodes must be encrypted. However, due to the heterogeneity of the IoT systems, some nodes might

be able to embed general-purpose microprocessors for this task. In addition, low resources and constrained devices can only embed application-specific integrated circuits. Therefore, conventional cryptographic primitives are not suitable for low-resource smart devices due to their low computation power, limited battery life, small size, small memory, and limited power supply. As a result, lightweight cryptography may be an efficient encryption for these devices. Trust management is another security mechanism that detects and eliminates malicious nodes and provides secure access control. Automated and dynamic trust calculations are needed to validate the trust values of the participating nodes in an IoT network. The majority of trust management schemes focus on detecting malicious nodes; only a few trust-based access control methods have been proposed. In fact, with scalability and the large number of smart things storing sensitive data, there is an urgent need for automated, transparent, and easy access control management so that different nodes/users can be granted different levels of access. From another perspective, Blockchain technology can be used to create secure virtual zones where things can identify and trust each other [77]. Self-organization Blockchain Structures (BCS) can also be planned to set up the relationship between Blockchain and IoT, as suggested in [78].

- *Anomaly Detection in Sensor Systems:* The type of data that flow through the IoT system can vary to a great extent, in terms of either format, shape (in time and space), and semantics. Therefore, the process of separating normal from abnormal sensed data is extremely demanding. In the context of IoT applications, sensors are the real source of big data, which suggests that anomaly detection at the edge could be a powerful tool to address the inevitable data communication bottlenecks. Anomaly detection is concerned with identifying data patterns that deviate remarkably from the expected behavior. This is critical in the process of finding out important information about the IoT system's functioning, detecting abnormalities that are often rare or difficult to model or, otherwise, to predict [79]. A timely identification of anomalies is vital to preventing IoT system failure.
- *Advanced Techniques in Smart City Networks:* Artificial intelligence (AI), machine learning (ML), and deep reinforcement learning (DRL) play a key role in the evolution of the smart city sectors [80]. These techniques are now being developed as solutions for completely automated IoT applications. Using these techniques, the optimal analysis of the big data is performed to reach an optimal decision. Utilizing DRL/ML approaches can improve security; decrease energy consumption; reduce latency; and increase precision and accuracy in surveillance, energy management, air quality prediction, person detection, traffic management, etc. For example, an intelligent transportation system is highly based on ML- and DRL-based techniques to realize self-driving vehicles and guarantee the security of connected vehicles. DRL techniques are also used to precisely monitor and estimate the real-time traffic flow data in an urban environment. In SGs, big data analytics and thus the aforementioned techniques can enhance the safety of power grids, decision-making of power-sharing, management, and power grid performance. In particular, SGs are making effective use of smart meter big data for different applications such as load assessment and prediction, baseline estimation, demand response, load clustering, and malicious data deception attacks. In health intelligence, extensive use of AI, ML, and DRL techniques is implemented due to high-performance IoT devices, Cloud Computing, and an increase in data rates. These techniques can play a vital role in disease diagnosis, cure prediction, social media analytics for a particular disease, and medical imaging [81]. In cyber-security, the role of AI-, ML-, and DRL-based techniques is also outstanding. These techniques can be used from an advanced security perspective of IoT to confront security threats. Notably, the accuracy and precision of the aforementioned techniques can be further enhanced by increasing the amount of training data to strengthen their learning capabilities and hence the automated decision efficiencies [82].

4. Protocols Used for SCAs

Figure 3 shows a proposed taxonomy of networking protocols and architectures for SCAs. It also shows the challenges in IoT communications via TCP/IP.

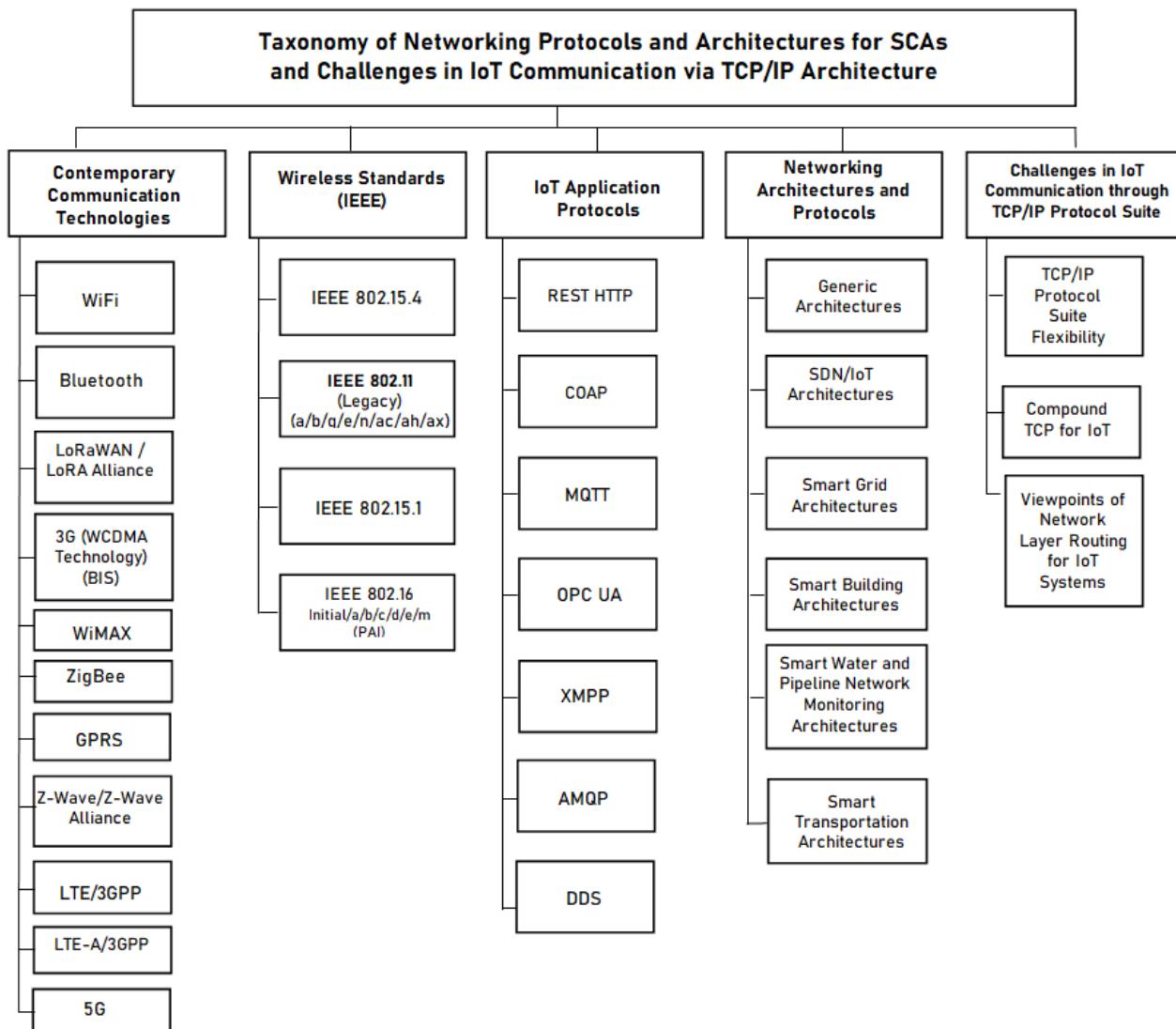


Figure 3. A taxonomy of technologies facilitating communication and networking for smart cities with IoT-enabled application protocols and suggested networking architectures and protocols.

SCAs involve numerous smart things that operate on low-powered battery devices [83]. New connectivity solutions are being investigated in light of the following question: do the currently available methods, tools, and techniques—especially those for wireless networks—allow for the reliable handling of such a large number of smart devices?

Yaqoob et al. [84] provided details on current connectivity solutions based on WPAN technologies such as ZigBee, WiFi, Bluetooth, and others that offer low-power D2D communication. In these technologies, the throughput performance, the number of connected devices, transmission ranges, etc., are severely constrained. Other technologies (e.g., WiMAX, LTE, and LTE-A) involve significant power consumption and are only partially applicable to such settings. IEEE and 3GPP adapt their technologies and communication strategies to the rapidly expanding IoT-based modern communication perspective. IEEE 802.11 (WiFi) was initially designed to maintain higher throughput performance for fewer stations distributed over a shorter distance in an interior context. Due to the limitations of its initial design, this standard does not support IoT applications. Hence,

to enable IEEE 802.11 adaptive in such circumstances, the community (IEEE 802.11ah Task Group (TGah)) developed a new power-efficient protocol [55]. They aim to create a system that enables effective communication between several indoor and outdoor devices. Nevertheless, the real-time implementation of IEEE 802.11ah may need to be improved by the absence of an appropriate interference mechanism.

IEEE 802.15.1 (Bluetooth), IEEE 802.15.4 (Zigbee), IEEE 802.11 a/b/g/n, Cellular 3G/4G/5G/LTE/LTE-A, and IEEE 802.16 (WiMAX) are only a few examples of standards and protocols that should be evaluated for their applicability for various SCAs. Smart home automation systems, smart buildings, and smart garbage systems require short-range communication capability and can utilize protocols (e.g., Bluetooth and Zigbee) from the WPAN group. These protocols are distinguished by a lower bandwidth requirement, minimal power usage, and a shorter-range communication infrastructure environment. In contrast, LAN groups such as WiFi can be used for SCAs that require longer-range communication. Such applications are smart transportation management systems.

The protocols from WAN groups, such as Cellular and WiMAX, can be adopted by applications that need wide-range communication, such as smart emergency response systems, weather and air quality monitoring systems, and smart grid systems. These features designed in terms of standards or protocols have enough capability that allows for both synchronous and asynchronous data connections. The best-effort traffic (which can effectively tolerate latency) allows the asynchronous data connections feature to be linked with smart city services or applications. Meanwhile, exploring synchronous data connections is possible for those services or applications that generate traffic mandating strict QoS standards such as low latency and high accessible network capacity [49]. Since IEEE 802.15.4 (Zigbee) is a short-range (low bit rate) communication protocol that often suggests higher flexibility for small devices running on low power, such a protocol can significantly increase network lifetime. Moreover, such a protocol encourages and indicates support for applications and services with relatively relaxed latency and throughput conditions in WPANs. The authors of [85] utilized a WSN based on IEEE 802.15.4 and proposed an intelligent system for lighting applications. The authors highlighted the benefits of using wireless emulsions: uncomplicatedness in the implementation and deployment, relatively easier in expanding a network, and flexibility in the system due to the use of wireless technology, which supports the usage of heterogeneous devices in the same implemented and deployed structure. Furthermore, they emphasized the advantages of employing the same intelligent infrastructure for a variety of services, leading to more effective management, monitoring, and cost-effectiveness. For example, by including specific smart metering devices such as water or gas meters, the smart network or infrastructure (that was initially established to target smart lighting applications) can also be used for smart metering applications.

5G has just supplanted 4G with advanced access schemes called BDMA and FBMC multiple access, which was first launched in 2015. In the case of BDMA multiple access, an orthogonal beam is frequently used, meaning that resources can be distributed in parallel to each mobile base station by dividing the antenna beam in accordance with the position of the mobile stations to enable multiple accesses to the base stations. Successively, this helps in improving the capacity of 5G networks [86]. Specifically, the idea of moving towards 5G is based on current technology advancements and particularly on unique customer needs. Nonetheless, it is typically presumed that implemented 5G cellular networks should address noteworthy complications that are not successfully addressed by 4G, i.e., enhanced network capacity and data rate, lower End-to-End (E2E) latency, reduced cost, and consistent user QoE provisioning. In addition, massive and rapid growth in the number of highly developed connected devices leads to a sharp increase in network traffic and a widening range of applications with unique dynamic requirements and features. Gupta and Jha [86] studied numerous facilitators, such as choice or use of spectrum, massive MIMO, traffic and power management policies, offloading (local), and self-configuring and organizing networks, which can address these challenges effectively. Real-time managing and supervising in smart city scenarios will be conceivable these days thanks to 5G. 5G

ultimately targets some networking possibilities, i.e., ultra-Reliable and Low-Latency Communications (uRLLC), enhanced Mobile Broadband (eMBB), and massive Machine Type Communications (mMTC). In a smart city context, eMBB controls data transfer between a variety of networked user end devices, edge devices, or cloud servers. Conversely, mMTC aims to manage huge connected, complex devices, such as wearables, actuators, and sensors, through dense urban deployment. Finally, uRLLC takes responsibility for managing highly time-critical communication such as vehicular communication, base stations, and edge devices communication [87]. Although 5G has completely brought about a new revolution in the field of networking, numerous unknown challenges still are possible in these cases of communication when 5G is deployed in the context of smart cities. One major problem is power-efficient communication, especially when communicating low-powered battery devices such as sensors and other smart, complex wearables. Additionally, when two distinct technologies (4G/5G) work together, there might be a problem. Specific device-level compatibility problems might always persist when communication infrastructures migrate to next-generation platforms. Moreover, a big question arises, namely, how to handle the widespread use of gadgets, particularly those in isolated or difficult-to-reach places, as well as the potential high costs associated with building and maintaining 5G networks.

Table 2 compares protocols used for smart cities, while Table 3 evaluates standards utilizing features and characteristics.

Table 2. Comparison of protocols used for smart cities. Adapted and extended from [49,84,88].

Communication Technology/Standard ¹	Physical Layer Specifications		Data Link Layer Specifications ⁴	Data Rate ⁵	Coverage Area ⁶
	Operating Frequency Bands ²	Data Modulation and Receiver Sensitivity ³			
ZigBee/IEEE 802.15.4	2.4 GHz, 868 MHz–915 MHz (DSSS)	Data Modulation: 16-ary orthogonal modulation (2.4 GHz) and BPSK with DE (868 MHz–915 MHz). Receiver Sensitivity: –85 dBm (2.4 GHz PHY) –92 dBm (868/915 MHz PHY)	CSMA-CA, TDD (optional)	250 Kbps (2.4 GHz), 20 Kbps (868 MHz), and 40 Kbps (915 MHz)	30–50 m
Bluetooth/IEEE 802.15.1	2.4 GHz, 2400 MHz–2483.5 MHz (FHSS/FSK)	Data Modulation: GFSK and PSK (for higher data rates)–π/4 DQPSK and 8 DPSK Receiver Sensitivity: –70 dBm to –82 dBm (usually depends on the type of PHY use), say, Bluetooth LE 125K (Coded) PHY can achieve –103 dBm	TDD, M&S, FH	1 Mbps	1–100 m
WiFi/IEEE 802.11 (Legacy) (a/b/g/n)	Conventional: 2.4 GHz a: 5 GHz (OFDM), b: 2.4 GHz (DSSS), g: 2.4 GHz (DSSS, OFDM), n: 5 GHz (DSSS, OFDM)	Data Modulation: Conventional: DI, DSSS, and FHSS, a: OFDM b: HR-DSSS, g: OFDM, DSSS, and CCK n: OFDM using MIMO and CB Receiver Sensitivity: Legacy: 1 Mbps: –80 dBm, 2 Mbps: –75 dBm b: 2 Mbps: –80 dBm, 11 Mbps: –76 dBm g: 6–54 Mbps: –82 dBm to –65 dBm n: 1–54 Mbps: –80 dBm to –65 dBm	CSMA-CA	Conventional: 1–2 Mbps a: 6–54 Mbps (VMT) b: 1–11 Mbps (VMT) g: 6–54 Mbps (VMT) n: 1–54 Mbps (VMT)	1–100 m
WiMAX/IEEE 802.16	2.5 GHz, 3.5 GHz, 5.8 GHz (MIMO-OFDM)	Data Modulation: OFDM using MIMO, AMC, AAS Receiver Sensitivity: QPSK (1/2): –80 dBm, QPSK (3/4): –78 dBm 16 QAM (1/2): –73 dBm, 16 QAM (3/4): –71 dBm 64 QAM (2/3): –66 dBm, 64 QAM (3/4): –65 dBm	TDD, FDD	75 Mbps	1–5 Km (NLoS), 10–50 km (LoS)
LoRaWAN/LoRA Alliance	867–869 MHz (Europe) 865–867 MHz (India)	Data Modulation: LoRA (CSSM) Receiver Sensitivity: –137 dBm (SF = 12, BW = 125 kHz, NF = 6)	Pure ALOHA with DCLs or PSA (LBT)	250 bps–50 Kbps (Europe) NS (India)	2–5 km
3G (WCDMA Technology) (BIS)	1.92–1.98 GHz, 2.11–2.17 GHz (licensed)	Data Modulation: AM/PSK using QAM Receiver Sensitivity: –102 dBm	CDMA	384 Kbps (deployed)– 2 Mbps	1–10 km
GPRS	900–1800 MHz	Data Modulation: GMSK Receiver Sensitivity: –159 dBm	TDMA, FDMA, and FH	Up to 170 Kbps	1–10 km
Z-Wave/Z-Wave Alliance	900 MHz	Data Modulation: FSK/BFSK (for 9.6 Kbps and 40 Kbps) GFSK (for 100 Kbps) with BT = 0.6 Receiver Sensitivity: –104 dBm	CSMA-CA	9.6 Kbps–100 Kbps	100 m

Table 2. Cont.

Communication Technology/Standard ¹	Operating Frequency Bands ²	Physical Layer Specifications	Data Link Layer Specifications ⁴	Data Rate ⁵	Coverage Area ⁶
LTE/3GPP	2.5 GHz, 5 GHz, 10 GHz (OFDM CP for downlink, SC-FDMA CP for uplink)	Data Modulation: AMC, QPSK, 16QAM Receiver Sensitivity: -103 dBm (LTE/A signal—5 MHz BW, QPSK, CR = 1/3, SNR = -1 dB, NF of LTE/A-based receiver chain = 5 dB)	TDD, FDD	75 Mbps (UL) 300 Mbps (DL)	30 km
LTE-A/3GPP	2.5 GHz, 5 GHz, 10 GHz, 15 GHz, 20 GHz (OFDM CP for downlink, SC-FDMA CP for uplink)	Data Modulation: AMC, QPSK, 16QAM, 32QAM, 64QAM, 256QAM Receiver Sensitivity: -90.7 dBm (LTE/A signal—5 MHz BW, 16QAM, CR = 2/3, SNR = 11.3 dB, NF of LTE/A-based receiver chain = 5 dB)	TDD, FDD	500 Mbps (UL) 1 Gbps (DL)	30 km
5G (New Radio (NR) Air Interface) (Single Unified, 4G + World Wide Wireless Web (WWWW))	For 5G mmWave access, an extensive spectrum of bands between 13 and 86 GHz has been recommended C-band (3300–4200 and 4400–5000 MHz)	Data Modulation: UFM, F-OFDM, and FBMC 5G New Radio (NR) Uplink Receiver Sensitivity: $P_{\text{Ref}} = TN + 10\log_{10}(BW) + NF + IM + SNR$ At room temperature, the TN in a 5G system is $-174 \text{ dBm}/\text{Hz}$. For Wide Area BS, Medium Range BS, or Local Area BS, the base station NF is 5 dB, 10 dB, or 13 dB, respectively. IM = 2 dB. The SNR value is that at which 95% of the maximum throughput is achieved. $P_{\text{Ref}} = TN + 10\log_{10}(BW) + NF + IM + SNR = -93 \text{ dB}$, (For NF = 5 dB, BW = 100 MHz, SNR = -1)	TDD, FDD	10–50 Gbps	Depends on changing cell radius (1 km to several km's)

1: LoRaWAN: Long-Range Wide Area Network, 3GPP: Third-Generation Partnership Project, WCDMA: Wideband Code Division Multiple Access, BIS: Broadband Internet Service, GPRS: General Packet Radio Services, LTE: Long-Term Evolution, LTE-A: LTE-Advanced, 3GPP: Third-Generation Partnership Project. **2:** DSSS: Direct-Sequence Spread Spectrum, FHSS/FSK: FHSS: Frequency Hopping Spread Spectrum/Frequency Shift Keying, OFDM: Orthogonal Frequency-Division Multiplexing, MIMO-OFDM: Multiple-Input/Multiple-Output-OFDM, OFDM CP: OFDM with Cyclic Prefix, SC-FDMA CP: Single Carrier-Frequency Division Multiple Access with Cyclic Prefix. **3:** BPSK with DE: Bi-Phase Shift Keying with Differential Encoding, GFSK: Gaussian Frequency Shift Keying, PSK: Phase Shift Keying, $\pi/4$ DQPSK: $\pi/4$ Phase Differential Quaternary PSK, 8 DPSK: 8-Phase Differential PSK, DI: Diffuse Infrared, DSSS: Direct-Sequence Spread Spectrum, FHSS: Frequency Hopping Spread Spectrum, HR-DSSS: High Rate-DSSS, CCK: Complementary Code Keying, MIMO: Multiple-Input/Multiple-Output, CB: Channel Bonding, AMC: Adaptive Modulation Coding, AAS: Adaptive Antenna System, QPSK: Quadrature PSK, QAM: Quadrature Amplitude Modulation, CSSM: Chirp Spread Spectrum Modulation, SF: Spreading Factor, BW: BandWidth, NF: Noise Figure, AM/PSK: Amplitude-Modulation PSK, GMSK: Gaussian Minimum Shift-Keying, BFSK/FSK: Binary-Frequency Shift Keying, BT: Bandwidth-Time product, SNR: Signal-to-Noise Ratio, CR: Code Rate. **4:** CSMA-CA: Carrier Sense Multiple Access-Collision Avoidance, TDD: Time division duplexing, M&S: Master and Slave, FH: Frequency Hopping, FDD: Frequency Division Duplexing, DCLs: Duty-Cycle Limitations, PSA (LBT): Polite Spectrum Access (Listen Before Talk), TDMA: Time Division Multiple Access, FDMA: Frequency Division Multiple Access. **5:** VMT: Varying Modulation Types, NS: Not Specified, UL: UpLink, DL: DownLink. **6:** LoS: Line of Sight, NLoS: Non-LoS.

Table 3. Evaluation of standards utilizing their features.

Communication Technology/Standard ¹	Features ²	Topology ³	Network Category ⁴	Limitations
ZigBee/IEEE 802.15.4	It allows short-range transmissions. It requires lesser bandwidth and minimal power usage. It clears channel assessment (for the case of CSMA). Dynamic selection of operating channels for coexistence. Packet strength signal for effective forwarding and location. It is designed and suited for PAN-based applications.	Mesh	WPAN	Low data rate and short coverage.
Bluetooth/IEEE 802.15.1	It creates dynamic (ad-hoc) connections using radio waves. It presents low-cost, robust, low-power solutions for P2P communication. It allows for short-range transmissions. It is mainly designed and suited for PAN-based applications. It suggests support for IoT devices, via BLE (version), and conserves power by continually maintaining devices in sleep mode until they are connected. It helps with quick device pairing and reconnections, which improves device availability and operational efficacy.	P2P	WPAN	Short coverage and less secure.

Table 3. Cont.

Communication Technology/Standard ¹	Features ²	Topology ³	Network Category ⁴	Limitations
WiFi/IEEE 802.11 (Legacy) (a/b/g/n)	<p>General features: It can aid both in an infrastructure-mode and an ad-hoc manner. These standards are quickly utilized in temporary and permanent LAN installations and deployments because of their flexibility and performance. It supports network management service and asynchronous communication. It suggests time-constrained delivery services and support for broadcast and multicast services. Moreover, it offers support for long-range communication.</p> <p>Specific features: IEEE 802.11a—works on the 5 GHz band, has a lesser interference level than other devices but has higher propagation losses compared to the 2.4 GHz band. IEEE 802.11b—works on the 2.4 GHz band. There may be interference issues with those devices, which, too, operate on the 2.4 GHz band. However, it offers a higher capacity and reachability than the 5 GHz spectrum to get through obstructions. It can also provide support for the ARS method [79], which allows an IEEE 802.11b device to dynamically switch from its theoretical maximum data rate (11 Mbps) to lower data rates such as 5.5 Mbps, 2 Mbps, or even 1 Mbps if interference rises. IEEE 802.11g—faster operating speed and generally has better signal range, being not easily obstructed. The IEEE 802.11g-based devices used OFDM to carry higher data rates while providing robustness against multipath fading/effects. However, additional modulation techniques (as shown in Table 2) are also used to preserve and manage compatibility. IEEE 802.11n—offers superior performance to its other peer standards by suggesting modifications in MIMO, OFDM, power saving, antenna technology, and wider channel bandwidth. The IEEE 802.11n-based access point can operate in Legacy, Mixed, and Greenfield modes [89]. This standard effectively exploits MIMO to take complete benefit of the available data rate.</p>	Star	LAN	Short coverage, comparatively higher signal attenuation, less reliable and stable compared to wired connections.
WiMAX/IEEE 802.16	<p>It was introduced initially to overcome the disadvantages of mobile networks and WLANs. It supports high data transmission rates while allowing more coverage than WLANs. It provides numerous QoS scheduling mechanisms supporting heterogeneous traffic, such as VoIP, voice data (traffic), video data/streams, and Internet traffic. Moreover, it has specific features such as high-speed Internet; a long-distance communication facility; and support for security, mobility, and scalability.</p>	P2MP, Mesh	MAN	Not widespread and operationally expensive.
LoRaWAN/LoRA Alliance	<p>It provides long-range transmissions and offers robustness from interferences. The PHY layer of this standard or protocol modulates the signal in the SUB-GHz ISM band. This specification aims to provide low-power WANs with capabilities specifically required to facilitate low-cost mobile secure bidirectional communication. Additionally, it defines the idea of geolocation, which can be quickly applied to enable GPS-free tracking applications.</p> <p>It utilizes minimum amounts of power, and hence IoT-based sensors and actuators can operate for a long time. Additionally, it manages less bandwidth utilization, making it their default choice for IoT-based deployments.</p> <p>The overall architecture (i.e., star) is relatively straightforward since a LoRaWAN-based GW can be designed to manage numerous end devices or nodes. It also offers secure communication between the end device or node and the application server using the AES-128 encryption standard.</p>	Star	WAN	Short coverage.
3G (WCDMA Technology) (BIS)	<p>This MNWT was initially engineered and designed to transmit and receive multimedia traffic with variable and high bit rates. This standard (having a comparable spectrum everywhere it is used) enables seamless worldwide networking. It utilizes the packet switching concept for data communication and circuit (or optional packet) switching technique for voice communication. It allows global roaming across a similar type of network (wireless) called a cellular network at 384 Kbps or even higher (up to several Mbps).</p>	-	WAN	Spectrum licensed cost, huge power consumption, and insufficient bandwidth to handle growing user demands.
GPRS	<p>As an enhancement over GSM, GPRS adds several nodes called GSNs to support end-to-end packet-switched services in the system. It operates by aggregating several separate data channels by the concept of packetization. Moreover, it is a low-cost technology that suggests a packet-based radio service. It offers the capabilities such as a high transfer rate, volume-based billing, shorter access time, improved radio resource utilization, and simplified access to packet data networks [90].</p>	-	WAN	Low data rate.

Table 3. Cont.

Communication Technology/Standard ¹	Features ²	Topology ³	Network Category ⁴	Limitations
Z-Wave/Z-Wave Alliance	It allows for operation in the low-frequency range, hence offering better performance. It supports low-power mesh networks and employs BFSK modulation. The lower frequency with longer wavelength allows Z-Wave devices to establish more reliable and faster connections since these parameters assist these devices in easily penetrating objects and walls. Six layers of backward compatibility provide version interoperability. The interoperability facility among Z-Wave-based smart or conventional devices assists in blending several applications at once, such as HA, SA, and LA.	Star, cluster, mesh	WPAN	Difficulty in mobility management. Fewer security features.
LTE/3GPP	It is a 3GPP interface (radio) based on UMTS/HSPA and GSM/EDGE networking technologies. It suggests improvements in data rate and capacity by employing new and modified modulation schemes. Moreover, it offers support for FDM and TDM techniques. It adopts an IP-based network model that promises a seamless handoff of voice and data to cell towers using an older technology.	Star	WAN	High operational costs because extra antennas are used at network base stations to transmit data.
LTE-A/3GPP	Through modifying and proposing novel PHY layer specifications or implementations and reforming the CN, LTE-A offers much-improved performance over UMTS/HSPA MNwTs. It can speed up to 3 Gbps download and 1.5 Gbps upload. Additionally, it has various antenna systems that simplify switching between cell regions, as well as cutting-edge transmission techniques that pack more data per second into each hertz of the spectrum and improve throughput performance at the level of cell boundaries. Subsequently, it leads to superior performance in terms of consistent connection and capacity (network) [89,91,92].	P2P	WAN	The installation of towers to improve signals while a smart device is in motion may result in significant costs. Device compatibility is a concern because older models of devices that do not support 4G LTE cannot connect to LTE networks.
5G (New Radio (NR) Air Interface) (Single Unified, 4G + World Wide Wireless Web (WWWW))	This technology addresses significant challenges: a massive and quick increase in highly sophisticated connected devices contributes to a sharp escalation in network traffic and an expanding variety of applications with distinct dynamic demands and features. Since LTE user equipment is not required to be able to operate on an NR carrier, NR is designed to be optimized for performance without taking backward compatibility into account. Moreover, NR can support operations in licensed spectrum bands from below 1 GHz to 52.6 GHz with a spectrum expansion facility. In the case of mmWave frequencies, excellent capacity and high data rates are possible. This technology's ultra-lean design seeks to decrease interference and improve system power efficiency by effectively reducing always-on transmissions [93,94]. This technology utilizes sophisticated access procedures such as Beam Division and FBMC Multiple Access to adapt 4G to 5G networks. Beam Division Multiple Access (BDMA) schemes' central design principle is concurrently serving numerous mobile users. This technique typically uses an orthogonal beam, which suggests that resources can be allocated in parallel to each mobile base station by separating the antenna beam in accordance with the position of the mobile stations to enable numerous accesses to the base stations. This subsequently assists in improving the capacity of 5G networks [79].	E2E Network Slicing	WAN	In the case of the NLoS state, the effectiveness of this technology needs to be thoroughly examined, particularly when it runs at high frequencies because wireless channels' basic nature is inconsistent when the frequency changes to higher values. Due to higher frequencies' extreme vulnerability to interference from obstructions, this disadvantage exists. Subsequently, this hampers the throughput performance of underlying deployed Layer-4 protocols such as TCP and MPTCP.

1: LoRaWAN: Long-Range Wide Area Network; 3GPP: Third-Generation Partnership Project; WCDMA: Wideband Code Division Multiple Access; BIS: Broadband Internet Service; GPRS: General Packet Radio Services; LTE: Long-Term Evolution; LTE-A: LTE-Advanced; 3GPP: Third-Generation Partnership Project. **2:** CSMA: Carrier Sense Multiple Access; PAN: Personal Area Networks; P2P: Point-to-Point; BLE: Bluetooth Low Energy; LANs: Local Area Networks; ARS: Adaptive Rate Selection; OFDM: Orthogonal Frequency Division Multiplexing; MIMO: Multiple-Input/Multiple-Output; WLANs: Wireless LANs; VoIP: Voice over Internet Protocol; PHY: PHYSical; ISM: Industrial, Scientific, and Medical; WANs: Wide Area Networks; GPS: Global Positioning System; GW: GateWay; AES: Advanced Encryption Standard; MNwT: Mobile Network Technology; GSM: Global System for Mobile communication; GSNs: GPRS Support Nodes; HA: Home Automation; SA: Security Automation; LA: Lighting Automation; UMTS: Universal Mobile Telecommunications System; HSPA: High-Speed Packet Access; FDM: Frequency Division Multiplexing; TDM: Time Division Multiplexing; CN: Core Network. **3:** P2P: Point-to-Point; P2MP: Point-to-MultiPoint; E2E: End-to-End. **4:** WPAN: Wireless Personal Area Network; LAN: Local Area Network; WAN: Wide Area Network; MAN: Metropolitan Area Network.

4.1. IEEE 802.11 Standards

Table 4 presents IEEE 802.11 standards and their features.

Table 4. IEEE 802.11 standards and their enhancements/features.

Standards (Year Released)	Enhancement(s)/Feature(s) *	Target
IEEE 802.11 (1997) (Original)	The standard and its amendments serve as the foundation for wireless network products bearing the WiFi brand. This signifies two raw data rates of 1 and 2 Mbps that must be transferred via DSSS and FHSS at 2.4 GHz in the ISM band.	Wireless Standard (basic)
IEEE 802.11b (1999)	This standard is intended to operate in the 2.4 GHz spectrum; however, the level of interference issues is higher when this standard-based device tries to interoperate with many other devices/standards operating on the same band. It can attain a theoretical data rate of 11 Mbps. Nevertheless, dynamic adaptations can be applied to the transfer rate subject to the current interference level and signal power to minimize the error rate (ARS Policy). Depending on the channel conditions, the raw data rates can be adapted to 5.5 Mbps, 2 Mbps, and 1 Mbps. Additionally, it provides somewhat simpler deployment processes (e.g., upgrading the current chipsets) as it demonstrates backward compatibility with the original standard due to the use of CDMA and DSSS (same as the original standard) [89]. The coverage indoor and outdoor ranges are 115 feet and 460 feet, respectively.	WiFi-1
IEEE 802.11a (1999)	Designed to operate on the 5 GHz spectrum and to have the least amount of interference compared to other devices. Depending on the needs, the raw data rates can be changed to 48 Mbps, 36 Mbps, 24 Mbps, 18 Mbps, 12 Mbps, 9 Mbps, and 6 Mbps. However, it can reach a theoretical transfer rate of 54 Mbps. The coverage indoor and outdoor ranges are 115 feet and 391 feet, respectively [89].	WiFi-2
IEEE 802.11g (2003)	Allows for device compatibility with devices that operate and follow IEEE 802.11b standards. It can also attain a theoretical transfer rate of 54 Mbps. In real-time situations, it can achieve a practical data rate of 24 Mbps. Nonetheless, when IEEE 802.11b-based devices are introduced into IEEE 802.11g networks, or when these heterogeneous compliant devices interoperate, the rate decreases drastically to accommodate IEEE 802.11b-based transmission speeds every time that the compliant device tries to communicate [89]. The coverage indoor and outdoor ranges are 148 feet and 296 feet, respectively.	WiFi-3
IEEE 802.11e (2005)	It specifies a set of QoS augmentations for WLAN applications through extensive amendments to the MAC sub-layer. It addressed QoS requirements by emphasizing two-channel access schemes: (1) the contention-based EDCA scheme and (2) the contention-free HCCA scheme. This standard, via EDCA, provides traffic prioritization support based on QoS classes (similar to differentiated services). Conversely, this standard suggests parameterized QoS (similar to integrated services) via HCCA. It also specifies enhancement over the conventional IEEE 802.11 power saver method (APS) and reduces the signaling load [95]. It is designed to operate at frequencies ranging from 2.4 to 2.4835 GHz or from 5.75 to 5.850 GHz. This standard also specifies that a high transmission rate may not be sufficient to meet the QoS requirements imposed by real-time audio, voice, video, and live-streaming applications. Following that, the provisions of traffic prioritization at the MAC sub-layer were insisted upon.	QoS improvements

Table 4. Cont.

Standards (Year Released)	Enhancement(s)/Feature(s) *	Target
IEEE 802.11n (2009)	<p>This standard was suggested while keeping the increased speed requirement in mind. Later, it was able to boost the attainable speeds of WiFi networks beyond what was possible with 802.11g. Achieving such high performance required several new features, including a modified OFDM scheme, power-saving mechanisms, antenna technology, MIMO, and wider channel bandwidth. Nonetheless, backward compatibility in the standard has been significantly affected (reduced) under exceptional scenarios.</p> <p>Whenever or not an old standard compliance-based device attempts to communicate with an IEEE 802.11g-based device in an 802.11g network, the network's operation, performance, and other capabilities suffer significantly. These standard-based APs can operate in Legacy mode (choosing one standard amongst 802.11a/b/g), Mixed mode (choose (out of 802.11a/b/g/n) and operate on heterogeneous conditions), and Greenfield mode (operate with a single (common) 802.11n altogether) [89]. It can reach a theoretical transfer rate of 600 Mbps. The coverage indoor and outdoor ranges are 230 feet and 821 feet, respectively.</p>	WiFi-4
IEEE 802.11ac (2013)	<p>This standard (called initially VHT) was suggested while keeping increased speed requirements in mind (likewise with other standards). This standard was later able to increase the achievable speeds (up to 1 Gbps (minimum) to 7 Gbps (maximum)) of WiFi networks beyond what 802.11n was capable of. The standard enables the transmission of HD videos, online interactive games, live-streaming, and other demanding applications. It operates using MU-MIMO technology, which enables a single AP and its antenna to send data concurrently to several devices. As a result, this helps to increase airtime efficiency so that every associated client—regardless of the 802.11 types it operates on—finally receives the amount of airtime it is supposed to receive, depending on the technology used.</p>	WiFi-5
IEEE 802.11ah (2017)	<p>Designed to operate on unlicensed spectrum below 1 GHz, it can provide significantly more transmission coverage than traditional 802.11 standards, which typically operate on 2.4 and 5 GHz bands. This standard can be employed in those scenarios where accessible bandwidth is comparatively narrow. It can normally apply with WiFi (outdoor) for performing CTO, large-scale WSNs (i.e., smart grid), and extended-range hotspots. Supporting a reasonably large transmission range/coverage property aids in managing large-scale networks where the number of devices may be much greater than what the conventional 802.11 standard can support. It advises that changes to the PHY and MAC layers be made to provide important improvements including energy-saving capabilities, support for accommodating a high number of devices, reliable media access techniques, and throughput performance improvement by using small frame formats [96].</p>	Extended coverage, low-power WLAN
IEEE 802.11ax (2021)	<p>This standard was proposed with the consideration of higher speed requirements. Later, this standard increased WiFi network achievable speeds above what was made possible by earlier standards. Specifically, it can offer support for a 10 Gbps data rate, consistency, and low power consumption. It operates using MU-MIMO and MU-OFDMA multi-user technologies, which enables a single AP and its antenna to send data concurrently to several end devices. Although the 802.11ac standard is where MU-MIMO technology was first introduced, 802.11ax now allows for groups of up to eight clients. In addition, this standard also suggests several improvements in spatial reusing policies and power-saver schemes [97].</p>	WiFi-6

* ARS: Adaptive Rate Selection; CDMA: Code Division Multiple Access; DSSS: Direct Sequence Spread Spectrum; EDCA: Enhanced Distributed Channel Access; HCCA: HCF-Controlled Channel Access; APSD: Automatic Power Save Delivery; APs: Access Points; MU-MIMO: Multi-User, Multiple Input, Multiple Output; VHT: Very High Throughput; CTO: Cellular Traffic Offloading; MU-OFDMA: Multi-User Orthogonal Frequency Division Multiple Access.

4.2. IEEE 802.15.1

The IEEE 802.15.1 (WPAN protocol) uses the 2.4 GHz spectrum and a master/slave time division duplex mechanism that operates smoothly in the 10 to 100 m range with a 1 Mbps data rate. This technology uses modest data rates for short-range services designed to use less power. Recent implementations of this technology include Bluetooth and Bluetooth Low Energy (BLE), offering IP connectivity to aid the IoT [98]. The deployment of services offered for tracking and localization devices is typically suggested by BLE-based devices, which are recognized as BLE beacons. These beacons produce a signal that other compatible devices can pick up between 50 and 70 m away. Using such a beacon promises greater indoor localization accuracy than other technologies such as WiFi or GPS. They can be used for a wide range of services targeted toward information dissemination, the launch of points of sale, user tracking, etc., thanks to this capability. Additionally, to provide specific services of interest, it is frequently required to combine the BLE technology with other technologies such as WiFi [99]. Originally, the aim of BLE technology (Bluetooth Classic Radio (BCR)) was to provide a continuous wireless connection, i.e., BlueTooth Basic Rate/Enhanced Data Rate (BT BR/EDR). It became the perfect option for the IoT since it permits connectivity and audio-streaming applications using brief bursts of long-distance radio, which lowers the battery consumption of mobile devices (because they need not be connected all the time). Using the idea of dual-mode chipsets and the new BLE specification, smartphones or regular phones can be linked to other heterogeneous devices (such as headphones) in BR/EDR mode. Otherwise, they can be connected to wearables in LE mode. A low-power radio called BCR, or BT BR/EDR, intends to broadcast data across 79 channels in the 2.4 GHz unlicensed frequency range. Wireless audio streaming is primarily made possible through BCR, which has evolved into the industry-standard radio protocol for in-car entertainment systems, wireless speakers, and headphones. BLE aims to transmit data over 40 channels in the 2.4 GHz unlicensed frequency range. To facilitate the deployment of dependable and large-scale device networks, BLE seeks to provide support for a wide range of communication methods, typically P2P; broadcast; and, most notably, mesh [100]. This unique Bluetooth feature can be used to create distribution and locating maps utilizing fingerprint templates for indoor device and user localization. Due to BLE's greater susceptibility to abrupt fading and substantial changes in received signal strength, it has been proven that using BLE is more efficient than using WiFi-based solutions [99,101]. However, Bluetooth technology has a problem with increasing power usage, particularly when its BR/EDR mode is used in an IoT context. This is because this mode allows the master nodes to continuously poll the slave nodes, even when there is no data transmission. The researchers [102,103] already brought up this issue, addressed it, and offered a variety of scheduling techniques for polling the slave nodes. Moreover, the BR/EDR mode reveals a lack of scalability that further restricts the performance of the system.

4.3. LoRA

The LoRa protocol was primarily used for WAN applications and operated as a low-data-rate, low-power technology on the sub-1 GHz spectrum that could go up to 10 km. LoRa communicates on three classes of bandwidth: 125, 250, and 500 KHz. Even while this technology can function at the largest bandwidth class, which further improves data rate, it still causes issues with high power consumption, a shorter communication range, and an increase in the likelihood of interference because it is free to operate in a wider frequency spectrum. This method is founded on the idea of spread spectrum modulation and a CSSM variant with a spreading factor ranging from 7 to 12. The transmission range will expand as the spreading factor's value rises, but the power consumption will rise as well. The CSSM utilizes complete allocated bandwidth, thereby making it resilient to channel noise and multi-path fading, but it does not differentiate the noise in the channel such as DSSS. In contrast to the FSK modulation approach, which normally identifies signals that are 8 to 10 dB above the noise floor, the CSSM feature enables this technology to sense, perceive, and capture signals that are 19.5 dB below the noise floor [103]. Its

architecture uses a star network topology and includes gateways and end nodes. In this design, end nodes are referred to as slaves and run on battery-powered devices with limited power, but gateways are thought of as powerful machines that gather data from slave nodes. Furthermore, LoRaWAN is a communication layer that operates on top of LoRA. LoRaWAN incorporates the basic LoRa criteria and suggests improved adaptability and suitability for low-power applications. This layer/technology has advantages over cellular technologies, which are expected to be battery hungry by the concept. In practice, LoRaWAN improved network features and functionalities by addressing the concept of a specialized server (network) and specifically defining numerous device types to meet the needs of each specialized application. Managed communication, packet filtering, and packet scheduling are all made possible using specialized network servers. LoRaWAN has also facilitated bi-directional-employed adaptive transmission power and rate, which aids in optimizing network performance in terms of power consumption and throughput. This technology can be employed for a wide range of applications, such as smart health nursing [104], traffic monitoring [105], agriculture monitoring [106], localization [107], and smart grid applications [108]. In particular, this technology is useful for non-latency-sensitive applications and those that call for extensive deployments. Haxhibeqiri et al. [109] and Adelantado et al. [110] emphasized that LoRaWAN is feasible for smart metering, tracking, and localization-based applications. At the same time, it is not so feasible for real-time monitoring and video surveillance.

4.4. WiMAX

WiMAX can handle high capacity, i.e., a potential peak data rate of 60 Mbps for an entire downlink operation and a rate of 28 Mbps for an entirely uplink operation, based on the original IEEE 802.16 air interface standard (2004) [111] and the IEEE 802.16e amendment [112]. It can be done using two antennas with a channel bandwidth of 10 MHz. Additionally, it may provide support for multimedia services with different traffic characteristics and wide area mobility with changing QoS needs. Additionally, it offers a variety of QoS scheduling options for accommodating heterogeneous traffic, such as Internet data traffic, VoIP (Voice over IP), classic audio traffic, and voice and video streams [113].

Table 5 shows the specified WiMAX standards and their operational parameters [114]. This standard provides a communication channel between geographically separated devices. As a result, the maximum achievable covered distance ranges between 30 km and 100 km. However, this technology has some drawbacks, such as high installation costs and the possibility of complications and irregularities when dealing with high-definition multimedia traffic.

Wireless network traffic has recently increased extraordinarily due to the rapid proliferation of smart handheld devices, sensors, and actuators. These devices, along with smart controllers, mobile users, and other smart services-based specialized devices, are the most common use cases for W-LANs in dense network environments. In such a dense network environment, interference is a critical issue that must be addressed if satisfactory performance and, thus, proficient spatial frequency reuse is required. Subsequently, the standards IEEE 802.11 were designed and implemented to support these requirements. Numerous international organizations, including IEEE and 3GPP, adopted and improved their technologies in response to changing needs and the emerging IoT market. For instance, the original IEEE 802.11 (WiFi) standard was designed to support and provide superior throughput performance to a small number of stations located close to each other, and as a result, this technology was not particularly useful for IoT systems. As a result, to address the challenges and requirements of IoT, the IEEE 802.11ah Task Group (TG) was formed by the IEEE 802.11 MAN/LAN Standards Committee to redesign and extend the applicability of WiFi standards to IoT scenarios. They focused on the critical issue of power-aware efficient schemes and protocols to extend the functionality and applicability of 802.11-based networks while dealing with a variety of small power-constrained smart outdoor and indoor devices [55,97].

Table 5. WiMAX standards and their operational parameters.

Specific Standards	IEEE 802.16 (2001) ¹	IEEE 802.16a (2003) ²	IEEE 802.16b ³	IEEE 802.16c (2002) ⁴	IEEE 802.16d (2004) ⁵ (Fixed)	IEEE 802.16e (2005) ⁶	IEEE 802.16m (PAI) ⁷
Operating Frequency Band	10–66 GHz (LS RF Bands)	2–11 GHz (LS/ULS RF Bands) (WMANs)	5–6 GHz (ULS RF Bands)	10–66 GHz	2–11 GHz (LS/ULS RF Bands)	2–6 GHz (LS RF Bands)	450–3600 MHz (LS/ULS RF Bands)
Data Rate (max)	32–134 Mbps (28 MHz)	75 Mbps max, 20 MHz channelization	75 Mbps	70 Mbps (20 MHz)	75 Mbps	90 Mbps	100 Mbps (MA) and 1 Gbps (FA)
Coverage Area (Max)	10–50 Km	45 km	45 Km	50 km	45 km	100 km	100 km
Propagation model (Channel Condition)	LoS only	NLoS	NLoS	LoS	LoS/NLoS	NLoS	NLoS
Channel Bandwidth	20, 25, and 28 MHz	Selectable between 1.25 and 20 MHz	10, 20 MHz (5 MHz is optional)	28 MHz	Selectable between 1.5 MHz and 20 MHz		5–20 MHz/RF carrier, CA-supported feature to assist in attaining BW up to 100 MHz.
Mobility Support	Fixed	Fixed	Fixed	Fixed	Fixed/nomadic	Portable/mobile version of WiMAX	Portable/mobile version of WiMAX.
Topology (MAC Architecture)				P2MP and Mesh			
Assistance	More extended coverage than WLANs while sustaining high transmission rates	VoIP	Licensed exempt applications. QoS support.	Creating profiles (systems) for 10–66 GHz will help with compatibility requirements for LoS broadband wireless access.	Technological fixes and minor modifications to 802.16a standard. The ETSI HiperMAN standard was matched with this standard to enable worldwide adoption.	Mobility (60–120 km/hr) facility to WiMAX. Better adaptability and improved QoS support.	Many additional service classes. Increases mobility (350 km/hr), and guarantees superior QoS services.
Modulation Techniques Employed	QPSK, 16-QAM, 64-QAM	BPSK, QPSK, 16-QAM, 64-QAM	BPSK, QPSK, 16-QAM, 64-QAM	QPSK, 16-QAM, 64-QAM	OFDM, OFDMA, QPSK, 16-QAM, 64-QAM, 256-QAM, S-OFDMA	OFDM, OFDMA, QPSK, 16-QAM, 64-QAM, 256-QAM, S-OFDMA	OFDM, OFDMA, QPSK, 16-QAM, 64-QAM, 256-QAM, S-OFDMA
Access Scheme/Protocol				Request/Grant			
Salient Features	Overcomes the disadvantages of mobile networks and WLANs.	Designed to operate in the LS and ULS RF bands ranging from 2 to 11 GHz (to make it operable in low frequency ranges). As a result, gives WiMAX implementations more flexibility while maintaining data rate and transmission range.	Increases the amount of spectrum the technology may use in the 5–6 GHz RF channels and provides QoS support.	More specifics about this technology were standardized, which promotes interoperability by encouraging more consistent implementation.	Comprises minor enhancements and fixes to 802.16a standard. This extension also makes system profiles for the 802.16a device compliance testing.	Designed to standardize communication between carriers' mobile devices and fixed base station, instead of between base stations and static receivers.	Designed to increase the mobility facility (typically more than IEEE 802.16e). Moreover, enables the use of numerous advanced antenna conceptions i.e., beamforming and MIMO.

1: LS: Licensed Spectrum, RF: Radio Frequency, LoS: Line of Sight, QPSK: Quadrature Phase Shift Keying, QAM: Quadrature Amplitude Modulation. **2:** LS: Licensed Spectrum, ULS: UnLicensed Spectrum, RF: Radio Frequency, WMANs: Wireless MANs, NLoS: Non-Line of Sight, VoIP: Voice over IP, BPSK: Binary Phase-Shift Keying, QPSK: Quadrature Phase Shift Keying, QAM: Quadrature Amplitude Modulation. **3:** ULS: UnLicensed Spectrum, RF: Radio Frequency, NLoS: Non-Line of Sight, BPSK: Binary Phase-Shift Keying, QPSK: Quadrature Phase Shift Keying, QAM: Quadrature Amplitude Modulation. **4:** LoS: Line of Sight, QPSK: Quadrature Phase Shift Keying, QAM: Quadrature Amplitude Modulation. **5:** LS: Licensed Spectrum, ULS: UnLicensed Spectrum, RF: Radio Frequency, LoS: Line of Sight, NLoS: Non-Line of Sight, OFDM: Orthogonal Frequency Division Multiplexing, OFDMA: Orthogonal Frequency Division Multiple Access, QPSK: Quadrature Phase Shift Keying, QAM: Quadrature Amplitude Modulation. **6:** LS: Licensed Spectrum, RF: Radio Frequency, NLoS: Non-Line of Sight, P2MP: Point-to-MultiPoint, OFDM: Orthogonal Frequency Division Multiplexing, OFDMA: Orthogonal Frequency Division Multiple Access, QPSK: Quadrature Phase Shift Keying, QAM: Quadrature Amplitude Modulation. **7:** PAI: Progressed Air Interface, LS: Licensed Spectrum, ULS: UnLicensed Spectrum, RF: Radio Frequency, MA: Mobile Applications, FA: Fixed Applications, NLoS: Non-Line of Sight, CA: Carrier Aggregation, BW: BandWidth, P2MP: Point-to-MultiPoint, Orthogonal Frequency Division Multiplexing, OFDMA: Orthogonal Frequency Division Multiple Access, QPSK: Quadrature Phase Shift Keying, QAM: Quadrature Amplitude Modulation S-OFDMA: Scalable Orthogonal Frequency Division Multiple Access.

4.5. Challenges in IoT Communication Using the TCP/IP Protocol Suite

In IoT, smart sensing motes, devices, and actuators share unique features such as constrained memory, power, and processing capabilities; the need for facilitating real-time requirements of smart applications; extremely vulnerable radio environments; and little to no human involvement after deployment [115]. By enabling communication amongst these devices utilizing low-power-cost technologies, a new infrastructure for deployed smart services has been formed. Researchers [116] argued that the TCP/IP protocol suite might provide a solution and be flexible enough for a variety of evolving IoT communication scenarios. Unfortunately, there were additional challenges that network administrators, designers, and researchers had to overcome. Researchers were searching for the best way to install IPv6-based sensor motes that can effectively/minimally use the system's limited resources (i.e., power and bandwidth). Because of such power constraints, researchers highlighted the requirements of low-power Layer-2 technologies (i.e., BLE, IEEE 802.15.4) and low-power WiFi usage. In contrast with traditional Ethernet links, these technologies operate with smaller maximum transmission unit (MTU) sizes and slower transmission speeds. IoT network protocol designers faced a problem in adapting to and determining the ideal MTU size. Another obstacle is that IoT networks often are based solely on wireless networks and thus they can only communicate using wireless mesh technologies. This vulnerability brings extra challenges in front of TCP/IP architecture:

- (1) The current IP addressing model cannot assist mesh communication (since it relies on a multi-link subnet prototype) at all.
- (2) In mesh communication, the multicasting and broadcasting communication methods are quite expensive, power-demanding, and prohibitive as the network nodes are extremely power constrained. Moreover, unicasting is the only remaining alternative method.
- (3) Unicasting is power intensive in and of itself because it may take many hops while forwarding and may wake up an excessive number of nodes that are asleep. Notably, idle nodes and hops can modify the radio state's operation mode to save power. Additionally, a large amount of power is used and saved by a node during transmission, reception, overhearing, idle, and sleeping phases [117]. However, to ensure successful delivery, we cannot just alter the operational modes. Instead, it requires effective coordination and intricate synchronization [117,118].
- (4) There is a high requirement for scalable routing/forwarding schemes for IP communication to take place over mesh architectural systems.
- (5) For many IoT applications requiring data prioritizing and customized control, original TCP-suited features such as those operational on fixed MSS sizes (such as MTU sizes) that further lead to silly window syndrome or in-order byte-stream delivery to ensure dependability, are unsuitable [119]. Nonetheless, the IETF started defining standard Internet protocols such as RPL [120] for such specialized environments to minimize protocol overheads that impair the computing ability and memory management of these specialized resource-constrained devices.

WiFi-based infrastructure networks enable backhauling support, which helps establish and sustain seamless connectivity among smart IoT devices. In smart home wireless networks, this form of connectivity can be provided through TCP connections. The TCP/IP protocol suite supports dependable data delivery and congestion control strategies to maintain network throughput performance via TCP at Layer-4. TCP is a protocol that has been regularly modified and improved over the years to effectively transport large amounts of byte-stream in-ordered data via resilient P2P connections with comparatively lower latency needs. IoT services deal with atypical communication patterns, for which TCP/IP protocol suite-based protocols, such as TCP, are unable to handle such patterns adequately [119]. There are severe problems that TCP faces when it deals with an IoT application:

- (1) TCP connection establishment and termination (three-way handshaking) incur significant overhead in the system as most communication in an IoT application includes the transmission of brief segments and relatively little data.

- (2) TCP functionality needs resilient P2P connections. It is impossible to sustain these connections in an IoT network environment because smart sensors and other connected devices switch their mode of radio state from active to sleep phase persistently [119].
- (3) Some IoT applications might need broadcast and multicast communication patterns, and enabling such patterns via TCP will result in substantial network overhead in the entire IoT system and high-power consumption.
- (4) Some IoT services have very granular delay requirements, and any extra delay in the form of connection establishment or MSS creation (waiting for data to fill the entire MSS) is completely unacceptable for their performance. Thus, TCP is unable to provide much support for these IoT services.
- (5) IoT applications that rely on wireless communication scenarios must deal with critical wireless channel characteristics such as channel error, interference, and wireless interface properties that result in buffer-induced, channel-induced, link-layer contention-induced, and collision-induced packet losses. When TCP operates in such a setting, its stringent in-order delivery requirements and retransmission policies (i.e., fast retransmission) may occasionally result in very serious system problems such as Head-of-Line (HoL) or Receiver Buffer Blocking, which ultimately results in a reduction in throughput, delay, and power consumption performance [121–124]. Furthermore, wireless MAC methods that use MAC-level retransmissions may further impair TCP’s performance, if Layer-2 retransmission latency exceeds the TCP Retransmission Time Out timer.

Some standards, such as BACnet/IP [125], were proposed to implement Layer-4 functionalities at the Application Layer (AppL) itself and proposed to utilize UDP as an underlying Layer-4 protocol. Managing packet losses should depend on an application’s requirements, which may vary from application to application. However, TCP and its updated variants rely on the concept of data delivery deferment and try to perform retransmissions from an already created copy in the sender buffer. However, this is not the only approach to dealing with packet losses in the network. Another method is for AppL to accept packet delivery that is not completely flawless and proceed with its current operations. This feature will be helpful in real-time audio and video distribution. Additionally, retransmission is an additional option. However, AppL should handle this retransmission rather than an underlying Layer-4 protocol such as TCP. In terms of buffering the lost data bits, doing so enables the source application to reconstruct them. Furthermore, in situations where real-time services are severely constrained, the transmitting application may transmit fresh data instead of retransmitting lost data to “repair” the effects of the initial loss [126]. Clark and Tennenhouse [126] concluded these concepts and subsequently introduced the concept of Application Level Framing (ALF). Implementing Layer-4 facilities at AppL itself brings the idea of employing ALF into the system. Hence, utilizing the notion of ALF, a network can recognize individual Application Data Units (ADUs), and subsequently can offer support for flexible Layer-4 facilities, i.e., employing adaptive retransmission procedures for diverse forms of ADUs and disseminating data more effectively by using in-network caching. Unluckily, the TCP/IP protocol suite forbids applications from adding any application semantics into network-level packet structure. Therefore, it fails to provide support for the ALF scheme [119].

4.6. Compound TCP for IoT

Compound TCP [127] was initially designed to offer support for improved channel utilization and fairness performances. It will play a significant role in home networks with WiFi-assisted smart and standard devices [115,128].

Pokhrel and Williamson [115] studied the effectiveness of a compound TCP over an IoT scenario involving sensors and other devices (i.e., smartphones, laptops, PC, and home appliances). They analyzed and evaluated the scenario improving the performance of connections made using the examined TCP variant across infrastructure WiFi networks in the presence of significant buffer-overflow-induced losses and severely degraded transmission

channel circumstances. The authors also addressed the varying bandwidth requirements for all IoT devices as well as ubiquitous connectivity, ranging from traditional bandwidth-hungry Internet devices to low-power gadgets. The authors of [129] demonstrated a thorough evaluation of the steady-state performance of TCP via WiFi-assisted classical devices considering the situations of high-buffer-overflow-induced losses and significantly deteriorated transmission channel conditions. The authors of [115,129] suggested models that aided in capturing the dynamics of congestion and flow control of several concurrently running competitive long-lived compound TCP connections. In evaluating and developing these models, they considered MAC-level retransmissions, link-layer contention, channel failures, and collision. The authors of [130] utilized a transient model suggesting a new queue management scheme to capture the interactions of short-lived TCP flows (the most workable flows in IoT scenarios) over conventional traffic patterns over WiFi networks. However, the performance of TCP in WiFi networks is constrained, especially when using a single shared Access Points (APs). As a result, TCP might not be able to scale well and provide superior performance in wide-area Industry 4.0 networks, especially when wireless channels are often reused by several APs [131].

4.7. Viewpoints of Network Layer Routing for IoT Systems

The network architectures for IoT are heterogeneous and include WiFi, WSNs, Wireless Mesh Networks (WMNs), Vehicular Networks, and Mobile Communication Networks (MCNs) (5G/LTE/4G/3G) [132]. Due to the large-scale production of intelligent sensing devices, survivability and self-organization of deployed functional networks are essential. A WSN is deployed for a variety of smart agricultural, environmental, domestic, and military applications. It is an ad-hoc network with no infrastructure, in which the sensor nodes communicate over multi-hop routing. WSNs run on battery-powered, low-power sensors capable of sensing, collecting, processing, aggregating, and regulating communication. Numerous WSN-based platforms, including MICA2, TelosB, and MICAz MOTE, have been suggested. Therefore, some standards were introduced to enable interaction and other compatibilities among these numerous heterogeneous platforms. For example, the IEEE802.15.4 (Zigbee) standard creates the WSNs backbone as part of the IoT. WSNs provide critical functionalities for developing IoT systems, allowing Low-Powered battery-operated End Devices (LPEDs) with very minimal resources to attach to the Internet. A WSN can be considered a special form of LoWPAN consisting of several equipped sensor nodes. Due to the lack of IP communication infrastructure, *interoperability* must be obtained from the viewpoint of WSN and the Internet. To address the interoperability issue, various works suggested a standardized arrangement that could enable the usage of IP over LoWPAN. The IEEE 802.15.4 standard allows for the interoperability for Low power and Lossy Networks (LLNs). The design tenet of this standard outlines the physical and data link layers of the network and offers a low-cost framework for network operations. To link LPEDs to the Internet, 6LoWPAN may be used as an adaptation layer to enable sensors to implement an IP stack and become approachable by other conventional devices over the Internet. This adaptability layer also supports end-to-end connectivity, which enables a variety of applications and permits these LPEDs to implement routing and forwarding algorithms at the Internet layer. However, the current network layer routing policies cannot be supported when the number of nodes grows. Therefore, the RPL protocol [72] considers the LLN situation [133]. Most of the nodes in LLNs are resource-constrained, and they are connected by some lossy links that only support low data rates. These links are thought to be extremely unstable and have poor performance in terms of packet delivery rates. In such specialized networks, the traffic patterns are often P2MP and MultiPoint-2-MultiPoint (MP2MP) rather than just P2P [72]. These networks contain hundreds of smart devices. This makes the implementation of routing policies more difficult than ever. In addition, numerous existing traditional ad-hoc wireless network routing methods, such as DSR and AODV, cannot manage these unique situations and unforeseen circumstances. Designing and implementing routing in ad-hoc networking settings has been more difficult due to the

mobility aspect and the resource limitations at wireless nodes. Their forwarding policies' design principles emphasize QoS elements including bandwidth usage and end-to-end latency [134,135]. The forwarding rules frequently created and applied for WSNs situations take into account the increase in the network lifetime by effectively utilizing the node energy [117,136]. As these ad-hoc networks were designed to operate and maintain solely inside their operational infrastructure, this was very feasible. However, the interoperability of these ad-hoc networks is a major problem when such networks are integrated with IoT networks. The ad-hoc network integration with IoT needs novel routing policies that support scalability and assure QoS, fairness, and connectivity between two nodes (both in APs and ad-hoc networks) with the least amount of power consumption. The standard classical forwarding strategies were intended to ensure QoS between a pair of devices/nodes. In the case of an IoT environment, the routing procedures should suggest enough fairness so that each node can sufficiently get enough chances to communicate with nearby APs. For such specialized scenarios, hierarchical routing solutions are followed to decrease data redundancy and ensure data aggregation. Researchers have often raised concerns about the disadvantaged forwarding rules, which lead to the consumption of excess energy in networks while taking into account mobile and static ad-hoc network scenarios. It consequently increases the likelihood of frequent network disconnections, route failures, and even network partitioning, all contributing to the system's significant MAC-level and routing-level overhead problems [134,135]. Hence, bearing in mind the high-power consumption problem, many researchers presented numerous smart routing paradigms [118,134,135,137]. Still, many of these suggested schemes failed to achieve the desired QoS.

Cross-layer design-based recommendations for power consumption and congestion control are well-suited design proposals for comprehending the changes in wireless channel attributes. Therefore, significant work has been done in these areas. These designs provide support for dynamically accessing and evaluating extremely variable channel parameters at lower layers (MAC and PHY) for the Internet/Routing and Transport layers to further optimize forwarding and congestion window adaptations decisions [121,134,135,138–140].

The *Received Signal Strength Indicator* (RSSI) indicates how well a device can hear a signal from an AP or router. A network layer forwarding policy can effectively utilize the RSSI (accessible through lower layers dynamically) to assess link quality. AODV and DSR are examples of the traditional ad-hoc routing protocols used in various smart forwarding systems designed for IoT scenarios. The AOMDV IoT [141] and MLB [142] routing mechanisms were suggested for the IoT scenarios and talked about node and link disjoint paths while discovering routes. However, the proposed schemes do not shed light and discuss anything related to performance issues when there is a significant level of interference in the network because of traffic running parallel onto multiple paths. The abovementioned techniques do not always perform well in terms of throughput and end-to-end delay. Recently, the scheme [140] considered different critical factors such as interference level, link-layer contentions, routing load, MAC load, and other performance issues related to wireless scenarios. The authors of [140] insisted that multipath load distribution policies' efficiency depends on the distribution (physical) of routes. Nevertheless, different possible disjoint routes—those lacking any common nodes or links—might be able to interfere with one another due to the radio signals' predicted broadcasting behavior in wireless communication. Consequently, such separate disconnected pathways could be utilized to enhance the performance of the network as a whole [138,140].

When employing an IoT-based system, the end sensor nodes depend on WSN-based networking connectivity to deliver sensed and collected data from smart things to sink nodes. These nodes are commonly known as *IoT GateWay nodes* (IoT-GW). To balance energy usage and gather crucial sensor data, numerous such static and mobile IoT-GWs can be deployed in the system. In the whole system, numerous WSNs, gathering numerous types of critical data, are connected to the Internet [142,143]. Originally, Zigbee specified three forms of devices: Zigbee Coordinator, Zigbee Router, and Zigbee End Device, and

three forms of network topologies: tree, star, and mesh. Moreover, the Zigbee stack embraces AODV to create paths dynamically. In the case of star network topology, the Reduced and Fully Functional Devices (i.e., RFDs and FFDs) can communicate with the PAN central coordinator only. They are not capable of communicating with one another. Here, the PAN coordinator may be powered by mains, while the RFDs and FFDs run on low-powered limited battery devices. Moreover, in the case of the mesh network topology, any device can communicate to within-range devices at a point of time. Moreover, this topology contains a PAN coordinator, which can communicate with other RFDs and FFDs. Furthermore, this networking topology offers support for the usage of the integrated forwarding scheme united with hierarchical/tree and AODV routing procedures. Lastly, the tree (cluster) network topology is a subset form of mesh networking topology, consisting of RFDs and FFDs (which may act as coordinators). However, the FFD count could be more than the RFD count in the network. RFDs may attach to tree (cluster) network topology as the end nodes in the system. The coordinator FFDs can offer synchronization functionalities to other connected coordinators and devices. However, there will be a single PAN coordinator amongst these coordinators [144].

4.8. IoT Application Protocols

Each IoT application is based on IoT application layer protocols for data transfer. These protocols can be the following:

- *Representational State Transfer Hypertext Transfer Protocol* (REST HTTP): HTTP [145] is the primary client/server protocol that adopts the request/response model. HTPP has been related to the REST architecture [146] to ease the interaction between dissimilar entities over web-based services. The mixture of HTTP and REST enables IoT devices to make their status readily available in terms of the standardized CRUD (create, read, update, delete) functions [147]. The CRUD functions are mapped to the POST, GET, PUT, and DELETE techniques of HTTP, correspondingly. In this fashion, we can build a REST model for dissimilar IoT devices [148].
- *Constrained Application Protocol* (CoAP) [149]: It is a lightweight RESTful protocol lately standardized by the Internet Engineering Task Force (IETF). CoAP is used by IoT devices for IP-based, HTTP-like interactions. It uses UDP with acknowledgment messages to set up reliable communication based on a request/response interaction. It has reduced complexity, and thus it is suitable for resource-constrained IoT applications and machine-to-machine (M2M) communication.
- *Message Queuing Telemetry Transport* (MQTT) [150] is established for IoT messaging. According to MQTT design principles, network bandwidth and device resource requirements should be kept to a minimum while also aiming to assure dependability and some level of delivery assurance. Since June 2016, MQTT has been recognized by ISO as a standard (ISO/IEC 20922). The protocol continues to progress by formalizing popular capability options and adding new functionalities. The most recent version, MQTT v5.0, was released in 2018. MQTT operates according to a publish/subscribe paradigm. Clients connect to a centralized broker when using MQTT.
- *Open Platform Communications Unified Architecture* (OPC UA) [151]: This interoperability standard is used for the secure and reliable exchange of data in the industrial automation domain and other industries. It is platform independent and ensures the seamless flow of information among IoT devices from multiple vendors. It supports two different communication methods: the Client/Server method as well as Publish/Subscribe (e.g., over UDP or MQTT) to mainly meet different industry requirements from the production systems to edge and cloud scenarios. Today, the main IoT vendors including IBM, AWS, Google Cloud, Microsoft, and SIEMENS leverage secure, standardized information exchange in edge-to-cloud applications based on OPC UA.
- *Extensible Messaging and Presence Protocol* (XMPP) [152]: This extensible protocol is based on text messages that use XML (Extensible Mark-up Language), through which

it can implement both request/response and publish/subscribe methods by using suitable extensions. XMPP exchanges instant messages between clients, and this happens in real-time using a push mechanism to avoid increasing unnecessary network loads. XMPP also determines the state of an XMPP entity as online, offline, busy, etc.

- *Advanced Message Queuing Protocol (AMQP)* [153]: An open standard for passing business messages between applications or organizations using TCP. It connects systems, feeds business processes with the information they need, and reliably transmits onward the instructions that achieve their goals using the point/point and publish/subscribe interaction modes. AMQP was designed to achieve the main goals of message orientation; queuing; routing; security; reliability; and interoperability.
- *Data Distribution Service (DDS)* [154]: DDS was developed by the Open Management Group (OMG). DDS is a real-time M2M protocol that enables dependable, high-performance, interoperable, scalable data exchanges using a publish–subscribe pattern. DDS provides low-latency data connectivity, high reliability, and scalability in publish–subscribe and request/response patterns over TCP and UDP. The needs of various IoT applications requiring real-time data exchange can be addressed using DDS. Such applications are air traffic control, transportation systems, autonomous vehicles, and smart grid management.

Lastly, Glaroudis et al. [155] provided a comparison among IoT application protocols in terms of well-accepted key performance indicators and discussed their suitability in the framework of smart farming.

5. Networking Architectures and Protocols

5.1. Generic Architectures

Zanella et al. [37] provided an in-depth analysis of an urban IoT's enabling technologies, protocols, and architecture. They also demonstrated the implementation of an IoT island as a proof-of-concept in the Italian City of Padova. In the IoT, two methods provide data access to objects/things. The first involves deploying multi-hop mesh networks with short-range communication among network nodes using unlicensed frequency. The second involves using licensed frequency band long-range cellular technologies (e.g., 2G/GSM). Centenaro et al. [156] presented a hopeful alternative solution (i.e., a new type of wireless connectivity) called Low-Power Wide Area Networks (LPWANs). LPWAN is based on a star topology characterized by low-rate, long-range transmission technologies in the unlicensed sub-GHz frequency bands. The authors considered LPWAN to provide connectivity in the IoT scenario for a characteristic SCA. Furthermore, they discussed the advantages of LPWAN over well-known methods regarding effectiveness, efficiency, and architectural design. Leccese et al. [157] created a Raspberry-Pi Card-controlled SCA that uses a ZigBee Sensor Network and WiMAX to provide completely controlled street lighting. Sanchez et al. [158] described SmartSantander, an IoT experimental research facility that was deployed in Santander City, Spain. SmartSantander supports testing proposed protocols, services, and configurations in a realistic setting at an appropriate scale. Machine-to-machine (M2M) communication is a significant part of IoT. Vilajosana and Dohler [159] reviewed currently used smart city M2M technologies (i.e., sensors, data loggers, wireless modems, and gateway). They considered one of the most famous deployment use cases, i.e., smart parking. In any IoT environment for smart cities, a huge amount of M2M communication requests occur. Unfortunately, conventional network gateways cannot face this challenge. Huang et al. [160] presented an admission control model for M2M communications. Their model differentiates all M2M requests into delay-sensitive and delay-tolerant. Then, it aggregates all delay-tolerant requests by routing them into one low-priority queue, aiming to reduce the number of requests from various devices to the access point in the IoT for smart cities. Silva et al. [161] developed the bottom-up architecture after analyzing a variety of existing architectures. This architecture has four layers: sensing, transmission, data management, and application. Each layer integrates security modules to protect sensitive data. The sensing layer, located at the bottom of the

architecture, collects data from physical devices. The transmission layer is located above the sensing layer. Several communication technologies are used to transmit data from the transmission layer to the (upper) data management layer. The data management layer performs data fusion, data analysis, data processing, and data storing. It stores valuable information that various applications use at the application layer to provide services.

The majority of the above works mainly focus on a single characteristic, such as quality of service [162].

Marques et al. [163] proposed a generic, multilevel IoT-based smart cities infrastructure management architecture that allows the integration of physical objects, communication infrastructure, cloud platform, and IoT-based services in a pervasive way. This architecture (Figure 4) is generic and includes four layers: (1) Physical Objects, (2) Communication, (3) Cloud Platform, and (4) Services.

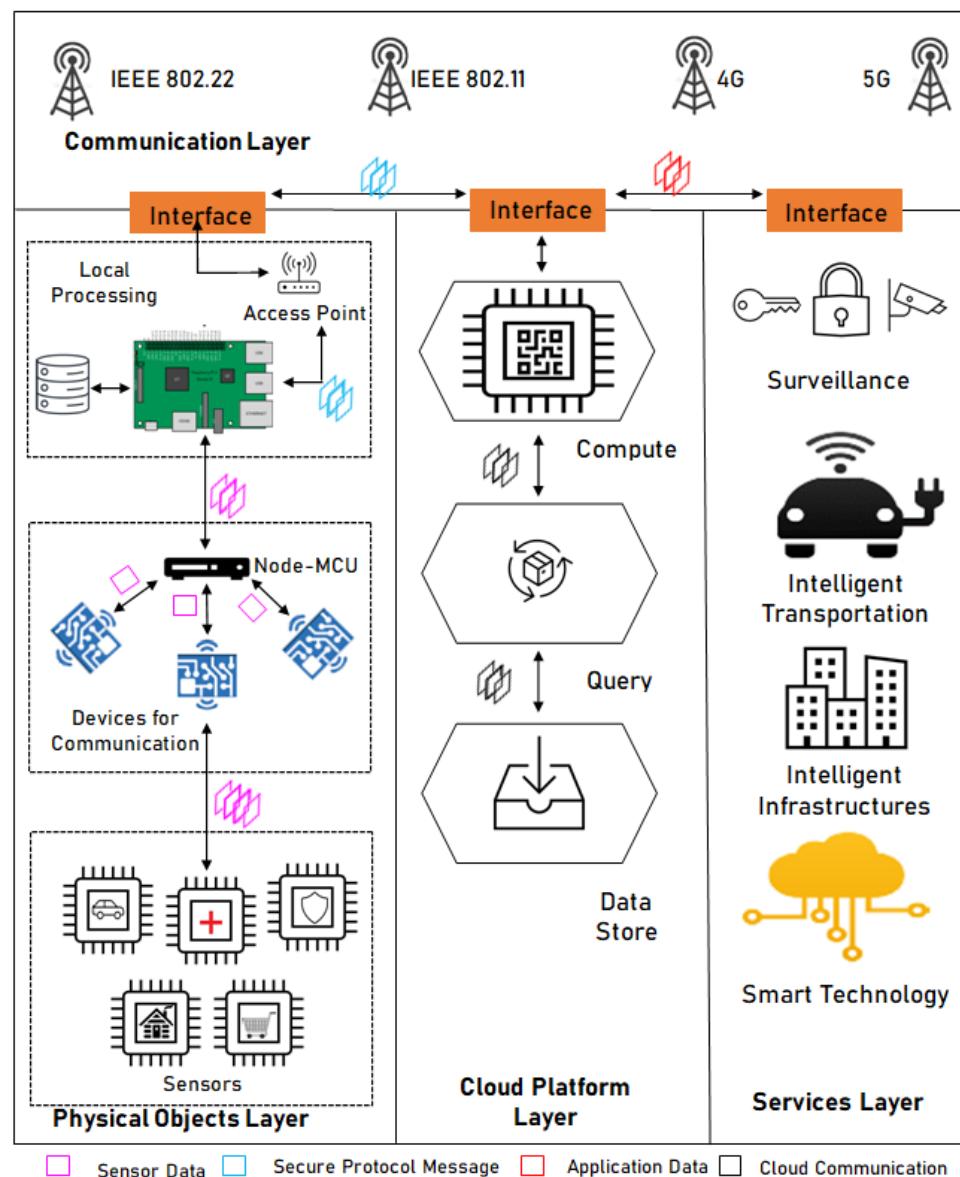


Figure 4. Architecture design. Adapted from [163].

1. The *Physical Objects Layer* enables IoT sensors to collect data that will feed the smart city architecture with information used to offer services. After the sensors collect data, a Communication Device is used to collect sensor data. A communication device can implement different technologies (e.g., RFID, Bluetooth, and Zigbee). Sensor data

are processed by a NodeMCU, which communicates with a Local Processing unit responsible for gathering information used by the application providing a service. The local processing unit brings elements of edge computing, as it pushes part of the computation to edge nodes instead of relying on concentrating all the computation in a centralized remote server.

2. The *Communication Layer*: The architecture supports a variety of network access technologies. The communication layer supports the implementation of various wireless technologies. The local processing unit located at the Physical Objects Layer defines the technology to be used and relays data to the communication layer using the interface of a network access point.
3. The *Cloud Platform Layer* provides three services: processing, database queries, and data storage. In the context of providing services for smart cities, each of these services can be dynamically allocated to satisfy the needs of various applications. Notably, only some applications and service types require a cloud platform to operate correctly. This layer is offered as part of the infrastructure provided, and its implementation is optional.
4. The *Services Layer* implements four groups, which are called classes of services: (I) Surveillance, (II) Transportation and Logistics, (III) Infrastructure, and (IV) Technology. In each class, different kinds of applications can be implemented to deal with the challenges of smart cities.

This architecture is a generic solution, so the underlying layers are designed to offer support to the applications. Therefore, it can be adapted to the specific implementation of a given service. To this end, the authors adapted their architecture to a waste management scenario.

Another multi-level smart city architecture [164] was built on semantic web technologies, and its design is mostly used in smart city wireless sensor network applications. Data collection, data processing, integration and reasoning, and device control and alerts make up its four layers. Using ontology, a data model, at the network's edge, Gheisari et al. [165] suggested a novel architecture for IoT devices in the smart city that protects privacy. Saadeh et al. [166] proposed a four-layer architecture for mobile object authentication in the context of IoT smart cities. Their architecture is based on the applicability of a proposed hierarchical elliptic curve identity-based signature authentication protocol. Naranjo et al. [167] presented a Fog-based smart city network architecture called FogC Architecture Network (FOCAN). To reduce latency and increase the efficiency of services among things with various capabilities, FOCAN is a multi-tier framework in which the applications operating on things collaborate to compute, route, and interact with one another through the smart city environment. One of FOCAN's primary benefits is that the IoT device can deliver services effectively and with less energy consumption.

5.2. SDN-IoT Architectures

Software-defined networking (SDN) [168] is an approach to enable flexible and efficient network configuration to enhance a network. SDN can provide many advantages for configuring city networks to support different applications. For example, SDN can improve the QoS of city networks against link failures [169] and meet smart city latency demands [170]. While some efforts are investigating this approach for supporting SCAs, there is room for developing more advanced management and networking mechanisms in SDN for efficient, reliable, and secure network configurations in smart cities. Jazaeri et al. [171] considered the advantages of integrating edge computing, SDN, and IoT technologies and reviewed different frameworks and platforms.

Liu et al. [172] proposed an architecture that decouples urban sensing applications from the physical infrastructure. In their architecture, centralized controllers manage physical devices and offer APIs for data acquisition, transmission, and processing services to develop urban sensing applications. Bi et al. [173] proposed a scalable SDN-enabled architecture that integrates a variety of smart city components and provides reliable and

timely scheduling for big data transfer to support smart city services. They also studied the time-constrained big data transfer scheduling (TBTS) problem under this architecture and proposed a heuristic with an intelligent scheme that can maximize the throughput and schedule the multi-flow transfer dynamically.

IoT systems collect and process data vulnerable to availability, integrity, and privacy threats. Nguyen et al. [174] proposed a collaborative and intelligent-network-based intrusion detection system (NIDS) architecture, namely, SeArch, for SDN-based cloud IoT networks. SeArch is a security architecture in which an arrangement of three layers of IDS nodes, i.e., Edge-IDS, Fog-IDS, and Cloud-IDS, is introduced with an effective collaboration among nodes.

Blockchain is an innovative solution for increasing data integrity and privacy in smart cities [175]. Sharma and Park [176] proposed a novel hybrid network architecture for the smart city by exploiting the strength of emerging SDN and Blockchain technologies. To achieve efficiency and address the current limitations, their architecture is divided into core and edge networks. By designing a hybrid architecture, their architecture inherits the strength of centralized and distributed network architectures. “PrivySharing” [177] is a Blockchain-based innovative framework for privacy-preserving and secure IoT data sharing in a smart city environment. This framework protects data privacy by segmenting the blockchain network into different channels, consisting of a limited number of approved businesses and handling a certain category of data, such as health, smart auto, smart energy, or financial information. Additionally, smart contracts contain access control rules that regulate who has access to the users’ data within a channel. In addition, private data gathering and encryption are used to further isolate and safeguard the data within a channel.

Islam et al. [178] designed a decentralized and distributed architecture for the IoT ecosystem that addresses the existing challenges through the use of the technologies Blockchain, SDN, and Network Function Virtualization (NFV). This energy-aware architecture confronts the problems of scalability, flexibility, complexity, monitoring, managing, and collecting IoT data and defends against cyber threats.

5.3. Architectures for Smart Grid

The automated and intelligent management of the next-generation electric power systems determines their effectiveness and efficiency. Smart Grid (SG) is the name given to the next generation of electricity systems, which are anticipated to offer various benefits over the current systems in terms of digitization, flexibility, intelligence, resilience, sustainability, and customization [179]. Smart transmission infrastructures use new technologies to improve power quality. Smart control centers monitor and communicate with electric devices remotely in real time, while smart substations self-consciously coordinate their local devices. The dispatch of electricity to end-users is implemented by using the electrical and communication infrastructures that connect the transmission and customer domains. The distribution domain includes distribution feeders and transformers to supply electricity. It interacts with much different equipment, such as distributed energy resources (DERs), plug-in electric vehicles (PEVs), automatic metering infrastructure (AMI), and sensors with communication capability. The distribution domain is responsible for delivering electricity to energy consumers, user demands, and energy availability. To provide quality electricity, the stability of this domain is monitored and controlled.

Typical applications [44] of the smart grid communications network are automatic meter reading, demand response, PEVs, substation automation, and DERs/microgrid. DERs are tiny energy production and/or storage devices linked to the distribution system. Distributed generation (DG), distributed storage (DS), or a combination of renewable and non-renewable sources are all possible sources for DER. Solar panels, wind turbines, combustion turbines, fuel cells, battery storage systems, etc., are a few examples of DER. An electric power system with one or more DER units and loads is referred to as a *microgrid*.

The communication infrastructure in the smart grid supports the capabilities of the smart grid and complies with performance standards. This infrastructure connects a huge number of electric devices and manages complex device communications. As a result, it is built in a hierarchical architecture with interconnected individual sub-networks, and each sub-network is responsible for separate geographical regions. The extremely dispersed smaller area networks that support the power systems at various locations are connected by WANs, which act as the communication's backbone. When the control centers are located a great distance from the substations or the end-users, the real-time measurements made at the electric devices are transported to the control centers through the WANs, and in the opposite direction, the WANs carry out the instruction communications from the control centers to the electric devices.

The authors of [43] present a communication architecture in an SG. This architecture includes (1) an energy smart house with electric appliances connected to the smart grid, (2) a residential complex with AMI, (3) a residential subdivision installed with solar panels, (4) a PEV charging station, (5) a power substation, and (6) power transmission lines. In this architecture, the Internet and ISPs serve as the backbone in connecting the distributed sub-networks. Demertzis et al. [180] presented and categorized the communication network standards that have been established for smart grids and should be considered in planning and implementing new infrastructures. Such standards are IEC 61850 for substation automation. This standard is based on open architecture and incorporates sampling and timing synchronization specifications based on IEEE 1588 in LANs and WANs [181]. Notably, IEEE 1588 is the standard for a precision clock synchronization protocol for networked measurement and control systems [182].

Due to the widespread use of renewable energy resources (RERs) throughout the power grid, it is anticipated that electric power distribution networks in smart grids would undergo significant changes to accommodate the nature of non-radial power flow. For the most part, the low-voltage distribution networks where RERs (such as solar cells) may be attached are not monitored by the majority of the present supervisory control and data acquisition (SCADA) systems for power grids. For the goal of active monitoring and control, Abd Rabou [183] presented a multi-hop wireless network with a cellular frequency-reuse structure that may supply the communication infrastructure to dense low-voltage distribution networks. A position-based QoS-aware routing protocol was also presented as a useful method for prioritizing data transfer across the newly introduced network architecture.

HetGrid [184] is a unique overlay network design with a specific QoS routing method for power distribution grid applications. It delivers QoS assurances across the network while taking into account three factors: bandwidth, latency, and dependability. The authors created two components to accomplish this:

- A multipath routing mechanism that compensates critical applications for their high-reliability requirements by using end-to-end physically disjoint paths, and
- Altruistic resource allocation with the QoS routing mechanism that targets communication with QoS guarantees for applications with strict QoS requirements.

The findings in [184] show that the HetGrid overlay network architecture enables extremely effective, trustworthy, and QoS-aware communication in heterogeneous networks.

The major characteristics that set SG apart from the standard electrical power grid are the ability to execute two-way communication, demand-side management, and real-time pricing. The present SG systems have interoperability problems because they need to be protocol independent. Therefore, global communication network management and monitoring approaches have been proposed using SDN [185]. Thanks to SDN, network administrators may more efficiently manage their networks by separating the control plane from the data plane. SDN has advanced in SG due to its reliance on communication networks. SDN implementation in SG systems has the potential to increase efficiency and resilience. SDN can assist the SG in integrating several SG standards and protocols by virtue of its programmability, protocol independence, and granularity capabilities to cope with varied communication systems. Rehmani et al. [185] presented SDN-based

SGC architectures, along with case studies. They discussed routing schemes for SDN-based SGC and provided a detailed survey of security and privacy schemes applied to SDN-based SGC.

Alam et al. [186] provided a detailed survey on smart grid communication networks in terms of communication network requirements, architecture, technologies, and applications. They proposed a Cognitive Radio (CR)-based Communication Network for Smart Grid. CR is a software-defined radio (SDR) platform that can quickly reconfigure its operating parameters, such as modulation/demodulation, compression algorithm, and error coding techniques, according to changing circumstances and requirements, through cognition. In such an SDR platform, radio transceivers can switch functions and operations on demand only. Molokomme et al. [187] reviewed architectures that aim to accomplish the various and strict QoS requirements in SG communication systems.

Wireless communication networks have been motivated to harvest energy from ambient environments and run energy-efficiently for economic and ecological benefits through improvements in the smart power grid and the advocacy of “*green communications*”. Hu et al. [188] examined recent developments in energy harvesting, redistribution, trade, and planning for future wireless networks integrating with smart grids. The authors considered the optimization of various energy-harvesting wireless systems as well as traditional models of renewable energy-harvesting technologies. Moreover, they discussed how to distribute redundant (unused) energy generated by cellular networks, plan for energy under dynamic pricing when smart grids are in place, and engage in two-way energy trading using smart grids.

From a different viewpoint, including IoT devices and providing connectivity, automation, and monitoring for such devices enables SG systems to sustain multiple network operations during the generation, distribution, transmission, and expenditure of energy. Numerous IoT-aided SG systems have been proposed in the literature. The survey [189] on IoT-aided SG systems considers the systems’ current architectures, uses, and prototypes.

5.4. Architectures for Smart Buildings

There are various building applications such as heating, cooling, load control, air quality, ventilation, lighting, water management, and cooking gas management. A smart building incorporates the major building systems on a common network and functionality to provide operational efficiency, fire safety, and security. A smart building architecture (SBA) manages several real-time domains, including automated temperature regulation, air cleaning, HVAC systems, and humidity control (i.e., indoor environment regulation and monitoring); smart lighting and controlling home appliances (energy management); a smart fire detection system; and other building operations. A typical smart building [190] has security cameras, lighting sensors, an indoor air quality system, a fire alarm system, a water management system, and an energy management system. Moreover, it can detect intrusion and supports HVAC services.

Diverse SBAs include complex operational systems, sensing, and communication technologies. Such architectures have converged into an IP-based architecture. This convergence is occurring rapidly with the increased usage of IP-based smart devices driven through IoT concerning conventional building management and smart buildings. Traditionally, numerous building systems utilized varied forms of networking protocols and cabling systems. This variety makes the whole system more complex and highly infeasible from both a deployment and a system administration standpoint [191]. SBAs entail making plans for and assisting with the inclusion of operational technologies that improve the application’s, service’s, or provision’s operational steps while also boosting the well-being of its users. Researchers, policymakers, and implementers should pay attention to several crucial issues, such as reliable communication/connection procedures, power-efficient measures, competent security measures, efficient sensors and actuators, and data analytics procedures. Amalgamating new systems and technologies with conventional (base) technologies to accomplish the revelation of SBAs, includes, but is not limited to, WSN

deployment; advanced power-aware traffic engineering policies; cloud, edge, and fog computing paradigms; big data engineering and analytics; and human–computer interaction procedures [192]. The rapid development of ICT technologies has enhanced the connectedness of intelligent sensing, actuators, and communication devices to real-time physical entities. Recently, smart sensing mechanisms, actuators, and data harvesting technology have boosted the area of SBAs proposals. However, choosing the best ICT technologies for a particular smart building domain poses significant difficulties, including heterogeneity of IoT devices and applications, workable networking protocols and architectures, power efficiency, and QoS/QoE provisioning [190,193]. One solution is the SDN paradigm, which manages the network more efficiently than a customary one. SDN also assists network services, including storage, routing, dynamic bandwidth management, and QoS. Hence, these simplifications offer a creative environment through the implementation of proper software tools for smart buildings. Network architecture and its implementation for intelligent infrastructure is based on IoT relationships (between IoT in home automation and applications) and can be established using smart home Cloud Computing based on SDN. Recently, Younus et al. [190] proposed an SDN architecture that improves critical SB parameters such as bandwidth efficiency, energy efficiency, latency, security, and reliability. Silva et al. [194] presented a Web of Things (WoT) SBA that is integrated with the representational state transfer (RESTful) application programming interface (API). The RESTful API employs HTTP requests (e.g., GET, PUT, POST, and DELETE) to access and use WoT data. Regarding network performance and smart building power management, the authors showed how their recommendation for smart city architecture improved performance.

Smart sensing devices and actuators permit collecting, monitoring, controlling, or modifying vital building parameters so that users receive the best QoS/QoE possible. These functionalities depend on sensor integration competence and their properties. These systems comprise signal conditioning circuits, implanted algorithms, power, and transceiver modules [195]. Researchers developed such system-based SBAs for assessing and regulating air quality, smart lighting systems, fire detection systems, power management, and other basic building operations.

An indoor-air-quality-based SBA considers sensing and actuator-based systems for monitoring and regulating air quality parameters. An indoor environmental observing system was initially suggested in [196] that observes polluting gases, temperature, and relative humidity. Other kinds of such systems have been proposed in [197,198]. Considering smart indoor lighting systems, numerous solutions have been proposed in the literature. In SBAs, light sensors manage and track the lighting system to satisfy the users' needs. The authors of [199] shed light on power consumption reduction via energy-efficient smart lighting systems. Today's smart building employs low-power usage LED-based light sources that last longer than Compact Fluorescent Lamps (CFLs) [200]. In reality, the development of control technologies, heterogeneous networks, and embedded systems has made it promising to create smart innovative lighting systems that can effectively address the problem of energy conservation. Researchers have recently begun testing by integrating different power-saving techniques in a single illumination system for improved energy efficiency while enhancing lighting performance without sacrificing user satisfaction. According to the authors of [201], using several cheap detectors, as opposed to a single expensive sensor, would result in improved performance and higher power savings. Considering the same motivation, various authors [202–204] have suggested similar types of smart lighting systems for several room types, such as classrooms and offices. In [205], the authors provide a deep and profound study concerning smart lighting systems focusing on power savings procedures and connectivity alternatives as well as the integration of visible light communication technology [206].

Recently, researchers focused on two main goals, namely, occupants' work performance and thermal comfort, to propose effective SBAs. Hence, many Occupant-Oriented Technologies (OOT) have been put forth by academics who want to maximize thermal comfort while conserving energy. OOT-based systems offer a practical way to lessen the

drawbacks of the automatic control used today. In practice, thermal comfort analysis is based on parallel objective and subjective evaluation. The objective evaluation comprises monitoring, assessing, and recording the status of environmental parameters through dedicated sensors and instruments following standardized guidelines. Subjective evaluation involves monitoring, assessing, and recording thermal preference, thermal sensation, and thermal environment acceptance. Further thermal comfort sensor results as the cumulative method to both above-mentioned analysis can be found in [193].

Green building refers to SBAs with an ambient intelligence system that adjusts to predetermined circumstances in real-world situations. In this situation, the system makes full use of embedded sensors in an environment that can gather data and subsequently allow the system to act in accordance with that data. The ambient intelligence concept aims to conserve natural resources with limited and efficient use of them to offer comfort to the occupants. Through unconventional energy sources, it also meets some of the conventional energy requirements [207]. Many aspects of SBAs, such as security, monitoring, and power efficiency, are the subject of extensive study. However, one of the most important functions of an SB system is to control the interior climate, which is typically done by HVAC systems [208]. The performance of HVAC systems in the instance of commercial buildings for frequency regulations has been demonstrated by the authors of [209] for this context. Their demonstrated numerical experiments suggest that 15% of rated fan energy can be employed for regulation use while having a minor effect on a building's indoor temperature. The method of computational control for passive and active sources was used in another scheme [210]. The authors emphasized the problem that the ambient and active sources of lighting, heating, ventilation, cooling, and shading are not synchronized in buildings. Such a computational control scheme is also suitable for reducing daily power usage. Similarly, numerous methods [211–213] considering HVAC systems have been proposed with respect to frequency regulation, predictive control, and smart controller.

An IoT-assisted HVAC smart system tracks environmental situations. It also notifies when measurements exceed thresholds and provides data on energy usage and consumption. In addition, it can autonomously turn equipment intermittently at programmed times. As individuals spend more time indoors (at home, work, or in other enclosed spaces) than outdoors, the air quality inside buildings should be improved along with that of the external surroundings. This is the task of indoor Air Quality Monitoring Systems (AQMS). The basic parts of an AQMS (Figure 5) are a sensor array, a processing/display unit, a signal conditioning circuit, a small amount of external memory, and a communication module that is typically wireless. A sensor array is a group of specialized micro-sensors that can detect certain airborne concentrations of gases such as NO_x, SO_x, CO₂, CO, and O₃, as well as some essential environmental parameters such as humidity and temperature. These sensors are connected to a GUI unit that shows the values of the real-time indoor air quality parameters and an external memory used to store real-time data [214]. When deploying such systems, various communication (wireless) modules, including WiFi, ZigBee, and LoRAWAN technologies, are considered.

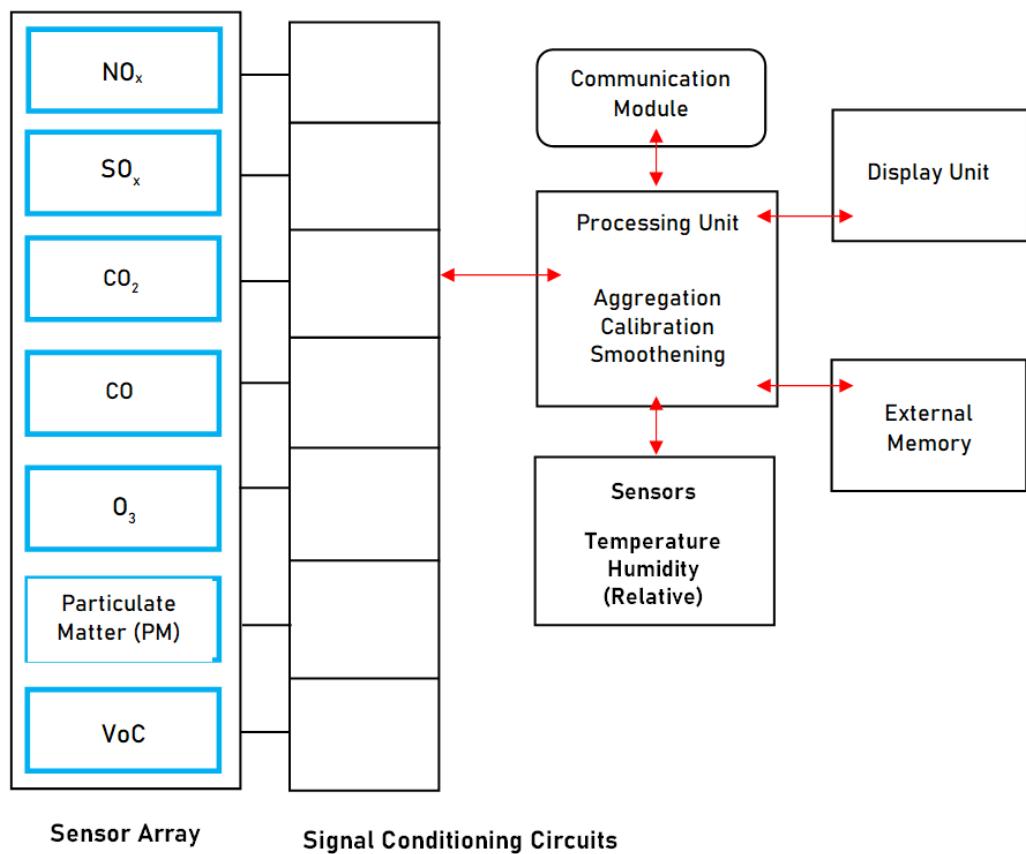


Figure 5. Air Quality Monitoring Sensor System. Adapted from [215,216].

Figure 5 shows a typical sensor system for an indoor environment for air quality monitoring.

Figure 6 shows an SBA architecture [217]. The system of this architecture collects vital information about the various air quality parameters, including CO_2 , CO, particles (Particulate Matter PM10 and PM2.5), and some other crucial parameters such as humidity and temperature. By using gas sensor boards and wasp motes, the authors created a method for collecting and monitoring the indoor atmosphere. For monitoring CO_2 and CO parameters, they also used TGS 4161 and TGS 2442 gas sensors. These sensors usually work using the resistive heating principle. The TGS 2442 sensor has excellent sensitivity to fluctuations in CO gas concentration. This sensor's internal resistance, or "IR", is inversely proportionate to the amount of CO present. As the CO content rises, the IR falls. While TGS 4161 also offers low power consumption and suggests better performance in detecting changes in CO_2 gas concentration, the TGS4161 is ideally suited for indoor air control applications as it can measure 350–10,000 ppm carbon dioxide. The authors used the DustTrak DRX, a specialized aerosol laser photometer that simultaneously measures mass and size fraction, for PM1 and PM2.5 monitoring purposes. To define and create an interface to the deployed sensor for wireless transmission of gathered aerosol data, this photometer is connected to a base station device via LAN. The authors also set up ZB (ENs) at each location that was taken into consideration, which sent updates on the air quality and aerosols at regular periods to BS (ZBC) that had already been set up.

This system assesses the indoor air quality to assess the current state of the indoor environment while simultaneously providing real-time inputs for HVAC system management. The authors also designed a toolkit that analyzes real-time air quality data and displays them through meaningful representations to service the SBAs. Likewise, Lozano et al. [216] proposed another IAQMS technique that considers a star topological architecture [217]. The ZB (ENs) in this technique is based on the XBee and XBee pro-version modules. Nevertheless, the suggested scheme [216] considers a single pollutant only, i.e., suggesting using

a GAC sensor. Conversely, the authors of [215] further claimed that they considered seven pollutants in their proposed implementation.

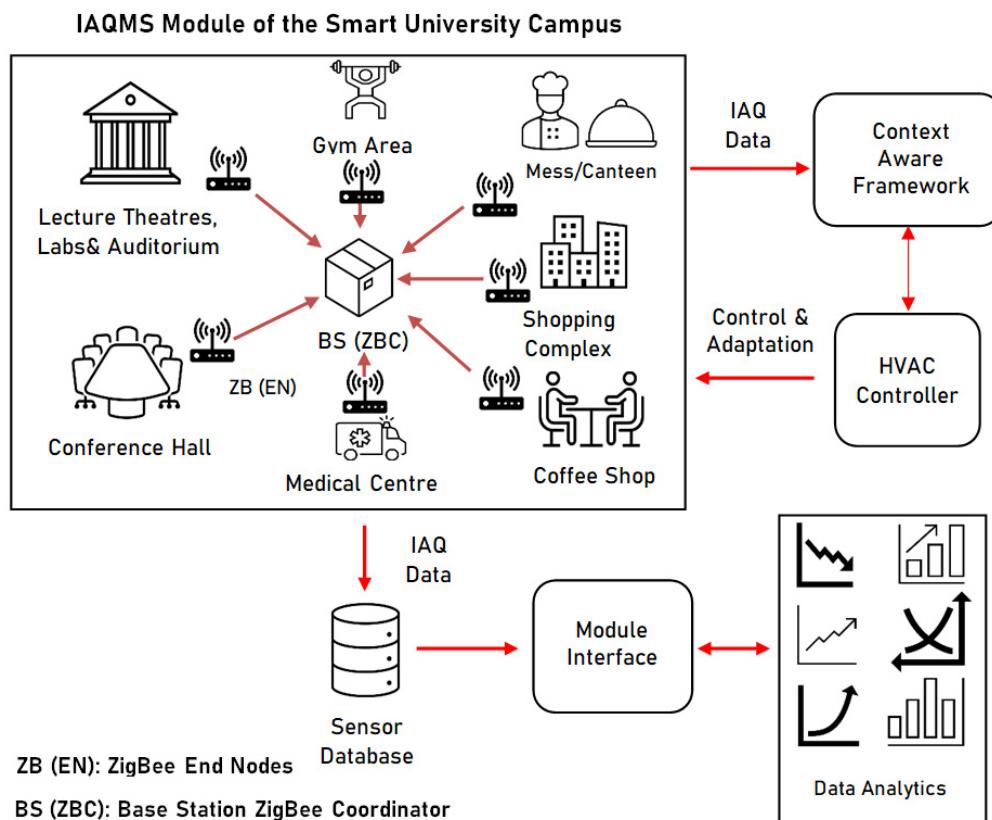


Figure 6. IAQMS architecture. Adapted from [217,218].

IoE for Smart Building: To achieve optimal functionality and energy-efficient performance, Kim et al. [218] offered an overview of the design and implementation of energy-related SB technologies, including energy management systems, renewable energy applications, and current advanced smart technologies. Undoubtedly, the electricity sector of smart cities is impacted by the Internet of Energy (IoE), which aims to increase energy efficiency, prevent energy waste, and enhance environmental conditions by integrating IoT technologies into distributed energy systems. Two examples of IoE technology are intelligent sensor use and the incorporation of renewable energy sources. As a result, the IoE is becoming a tool for legal science to support the goals of a smart city. Metallidou et al. [219] discussed the factors that prompted the European Union to create regulations to make it easier to transition current towns into smart cities, starting with existing structures. To achieve energy efficiency, the authors suggested a smart building template that uses IoT technology to manage the performance of all technical systems. In addition, they suggested an automated remote-control technique supported by a cloud interface to enhance the certification of existing buildings for energy performance. This technology reduces time-consuming processes and stores the energy performance of each building on a cloud platform to make decisions and put measures in place. A review of current tactics in the field of active building energy management systems (BEMS) was offered by Mariano-Hernández et al. [220]. The authors reviewed articles on several BEMS management techniques for residential and non-residential buildings, including Model Predictive Control (MPC), Demand Side Management (DSM), Optimization, and Fault Detection and Diagnostics (FDD). MPC predicts building response to control requests, while DSM is an agreement of actions to improve the energy system on the user side. FDD is an automatic procedure of detecting and separating flaws in BEMS to protect a system from additional harm. Moudgil et al. [221] examined cutting-edge academic and industrial

research to discover significant technological solutions that improve the integration of IoT in building infrastructure (BI). Their review also identifies key technical and non-technical problems that must be resolved through extensive research for BI to fully incorporate IoT. The authors contend that IoT in BI is still not operationally capable. IoT and BI stakeholders must make a concerted effort to give modern BI access to a generic IoT framework with cognitive intelligence and context-aware computing capabilities.

5.5. Smart Water and Pipeline Network Monitoring

Retrofitting the traditional water distribution system with smart devices has some benefits, including lower utility costs, lower consumer bills, and less water loss [222,223]. For example, smart water sensors can keep an eye on the pressure online and alert utilities to pressure changes or large pressure losses in the water network, allowing them to remotely adjust the pressure to save energy consumption [224]. Automation can be used for both operational procedures and components that provide functionality. For instance, when a water problem occurs during operation or with the element itself, the smart components inform the system center and then take action to avert a crash. The water utility can also determine a sensor's requirement for maintenance or replacement thanks to the automatic self-verification mechanism [225].

In [226], the authors suggest an IoT-based smart water grid architecture that includes technical systems, functions, and a hierarchy framework. Moreover, this smart water system (SWS) also comprises smart sensing mechanisms, simulation procedures, diagnostic techniques, disposal, warning, and control mechanisms. Although an SWS incorporates offline performance, real-time performance is defined by online procedures such as online data monitoring, online data assimilation, online modeling, online charting, and online results output. An SWS must have real-time functionality to implement the necessary smart features [227]. Researchers put a lot of effort [228] into developing water systems that operate intelligently. Real-time modeling, real-time sampling, real-time controlling, etc., which seek to reduce the lag between system input and system output, should be added to the smart performance of SWS. It was discovered that using SCADA would considerably increase the data transfer efficiency [229]. A smart water architecture [230] often includes five layers: (1) the physical layer; (2) the sensing and control layer; (3) the communication layer; (4) the data management layer; and (5) the data fusion layer. Within the framework of the GST4Water project, the authors of [230] presented a system that allows for receiving consumption data sent by a generic smart meter installed in a user's house and transferring them to a cloud platform. The consumption data are saved and processed to characterize leakage at the district meter area and the individual user level. Meanwhile, the processed data are returned to the Water Utility and can be used for billing. On the other hand, they provide regular feedback to the user, thus gaining full awareness of their consumption behavior. Panagiotakopoulos et al. [231] presented an IoT framework based on FIWARE that aims to realize a highly flexible standards-based open-source software solution for developing SWSs. They designed an architecture consisting of various FIWARE software components and two dashboard applications. Amaxilatis et al. [232] considered numerous intelligent infrastructure solutions regarding conventional water metering systems, which effectively facilitate uninterrupted bi-directional (whenever required) data exchange between water flow devices, metering equipment, and end-users. The authors' ultimate objective is to design, implement, and deploy more sophisticated infrastructure offering improved performance in bigger smart city infrastructure. To limit the amount of data that needs to be shared between the various system layers, their approach makes use of the FogC paradigm to develop the infrastructure for the smart water grid model.

The Information and Communications Technology (ICT) Solutions for the Efficient Water Resources Management project was funded by the European Commission under the auspices of the Seventh Framework Program (FP7). The goal of the Smart Water project is to examine the role of ICT in monitoring and effectively managing urban water systems,

with a focus on the deployment of sensors, communication technologies, and related decision support systems in utility providers' water networks to address issues such as leakage management, demand management, asset management, and so forth. Kulkarni and Farnham [233] focused on the issues surrounding wireless connectivity, proposed a framework for assessing potential solutions based on the total cost of ownership, and highlighted lessons learned from two European utilities' Smart Water case studies.

Pipelines are used to transport water, gases, and oil. Since they are frequently underground, the humid atmosphere easily erodes them, which may result in leaks. In addition, water in the pipelines may get contaminated by infectious agents or substances that are mistakenly or purposely introduced into the system. As a result, maintaining pipeline networks is crucial for maintaining public health and protecting the environment. The sensor node deployment profoundly impacts the sensing performance indicators for pipeline network monitoring, including coverage area, coverage population, and detection time. The sensor nodes should typically be positioned near the pipeline network's junctions [234]. Given the design of the pipeline network, the optimal sensor node deployment challenges are therefore formulated as integer optimization problems, where the integer variables represent the maximum amount of sensor nodes that must be placed at each junction. The deployment difficulties for pipeline network monitoring are typically challenging to solve because of the integer decision variables.

Pipeline network flows are not predictable. As a result, depending on the flow pattern, the sensing performance of a deployed sensor node may vary. As a result, the flow pattern is taken into account in [235], which formulates a mix-integer optimization problem to decide how to deploy sensor nodes to reduce the projected population at risk of malicious contamination. The authors solved the ensuing mix-integer optimization using a branch and bound technique. Even though a strategy such as this can identify the ideal answer, the time complexity is typically significant. This means that large pipeline networks cannot be used with the method. Similarly, the study in [236] considers the various demand patterns of water flows through pipes. The authors used a genetic-based method to find the best deployment locations to increase coverage under various monitoring station demand patterns. The global optimum of these heuristic algorithms could take a while to reach. The performance of the algorithms may also be impacted by their parameter choices. Consequently, we do not advise using it for massive pipeline networks.

Singapore's WaterWise@SG program aims to identify pipeline leaks and anticipate burst incidents [237,238]. PipeNet has also been put to the test in Boston to find pipeline leaks, where three tiers of nodes are employed to quantify pH levels and pressure. To reduce water waste, a system named IWCMSE [239] has been designed to track water consumption for businesses. A Steamflood and Waterflood Tracking System [240] has been created to find irregularities in pipeline systems, such as leaks and bottlenecks. With the aid of all these technologies, the investigators had the opportunity to evaluate the efficiency of the monitoring algorithms. However, these technologies rely on fixed sensors, and we still need to put innovative testbed models and systems built around crowd sensing and mobile WSN into place.

5.6. Architectures for Smart Transportation

The Internet-of-Vehicles (IoV, also known as V2X) aims to reduce traffic congestion and accidents. It also enables information exchange involving the vehicle and all entities that may have an impact on it. Vehicle networking and vehicle intelligence are the two technologies that underpin IoV implementation. The three components that compose vehicle networking are the onboard information service, VANET, and mobile network. VANET stands for vehicle-to-vehicle short-range communication. Providing remote location, remote diagnostics, navigation, and other information services is referred to as an onboard information service. Every car can be utilized as a potent mobile terminal thanks to mobile networks. Vehicle intelligence is the use of cutting-edge technologies, including artificial intelligence (AI), big data analytics, deep learning (DL), and cognitive computing

(CogC), to facilitate information sharing among people and vehicles, as well as between vehicles and the environment, infrastructure, or other vehicles.

Vehicular networks consist of data-gathering sensors and inter-vehicle communication systems. Such networks require an open and flexible layered architecture to handle characteristics such as interoperability, scalability, dependability, and modularity. Recently, the research community proposed efficient vehicle network architectures. For example, the Universal IoV (UIoV) architecture [241] includes seven layers. Offering services and choosing messaging protocols are tasks that fall within the application layer. Data preprocessing, big data processing, and intelligent transmission are all tasks that the multimedia and big data layer is in charge of. For IoV systems, the cloud service layer's ClCom and cloud virtualization technologies offer hardware computing platforms, infrastructure, and software services. In the UIoV architecture, the communication layer and the intra–inter devices layer are merged to accomplish the connectivity of many heterogeneous objects and networks. Notably, there is no intra–inter devices layer in classical architecture. The UIoV system's physical objects layer gathers and transmits all the data to the intra–inter devices layer for additional processing. In the IoV, both vehicles and non-vehicle items are identified using the Identification Layer.

Liu et al. [242] suggested another IoV network architecture to increase the flexibility of application management while enhancing the scalability and dependability of information services. This architecture has four layers in total, the data layer of which has a variety of nodes with various wireless communication interfaces. Because the topology of IoV is frequently changed, an immense quantity of data are frequently produced and transmitted at the data layer. To safeguard the accurate semantics of the underlying resources, the virtualization layer splits a few nodes into fog nodes and the network, computation, communication, and storage resources in IoV. To execute applications such as road safety management and data sensing, the control layer's SDN controller is responsible for scheduling the abstraction resources of the virtualization layer and interacting with the application layer. A difficult topic in network architecture design is dealing with diverse networks. Interoperability, scalability, dependability, and adaptability are some of its network features. The design seeks to increase layer separation and network architecture's total number of layers. In addition to being a service-oriented design, the IoV architecture should facilitate the connectivity of cars with heterogeneous networks and other communication devices. By introducing the CogC paradigm into autonomous driving systems, the learning ability of autonomous vehicles can be effectively improved. Utilizing both physical and network data space, the Cognitive Internet of Vehicles (CIoV) paradigm [243] improves network security and transportation safety. CIoV enables IoV to bear more accurate perceptive ability through cognition in the intra-vehicle network (driver, passengers, smart devices, etc.), inter-vehicle network (adjacent intelligent vehicles), and beyond-vehicle network (road environment, cellular network, edge nodes, remote cloud, etc.). The CIoV architecture includes a cognitive data engine that can conduct cognition of user tasks by the use of data collected, e.g., driving behavior model analysis, emotion analysis, and road condition investigation. Five layers are present in the network architecture of CIoV. The gathering and preprocessing of big data from several sources are done by the sensing layer. As opposed to the previous communication layer (of other architectures), the architecture's communication layer uses a cloud/edge hybrid structure to accommodate various application schedules. The data cognition engine at the cognition layer processes and interprets heterogeneous data streams (machine learning (ML), DL, data mining, etc.) using a variety of cognitive analysis approaches. The control layer's resource awareness engine is in charge of allocating and scheduling network resources with the aid of technologies such as NFV, SDN, network slicing, and self-organized networking (SON). There are primarily two categories in the application layer (i.e., usual application services and intelligent transportation applications).

Efficient message authentication and integrity are required to guarantee vehicle privacy and safeguard vehicular communications. To protect V2V and V2I communications

in the context of the VANET against a broad range of cyber threats, Karim [244] provided a cryptography-based routing solution. This solution includes a data encryption and decryption mechanism based on attributes and identity that has the lowest computational overhead while keeping the optimum level of security. Contreras-Castillo et al. [245] suggested a seven-layer network architecture. The user interface layer, which controls information exchange between the user and the vehicle, is the top layer. Utilizing roadside units (RSUs) and onboard sensors, the data collecting layer gathers data. The pre-processing and filtering layer eliminates the unnecessary information from the gathered data before sending the remaining information to the communication layer for transmission. Making choices and managing network service providers are the responsibilities of control and management. Large volumes of data must be processed by the processing layer to create the pertinent data needed for various applications. To stop assaults, the security layer directly manages each of the layers above. A unique network architecture with enhanced throughput, reduced latency, higher security, and widespread connectivity was recently proposed by Ji et al. [246]. This architecture consists of four layers:

1. *Security authentication layer*: The RSUs on the road may monitor traffic environment data in real-time after setting several sensors, surveillance footage, and radar. This layer determines the legality of the car and RSU that are requesting to join the network. Perhaps an illegal vehicle or an RSU that has been installed unlawfully will attempt to steal or alter the information of a real vehicle.
2. *Data acquisition layer*: This layer collects and categorizes many types of data from various networks. To ensure that the data can be sent to the edge layer securely, it digitizes the data.
3. *Edge layer*: Edge devices produce several data streams. As a result, processing and analyzing data in one go using ClCom will result in significant delays. As a result, we must process data more closely related to the data source. The edge node, a physical device situated closest to the data source, is used by the edge layer to carry out basic processing and analysis on the acquired local data. It releases data analysis findings for nearby traffic incidents and current road conditions in real-time, then creates a local decision-making plan, carrying out various ClCom jobs and boosting the cloud data center's computing power.
4. *Cloud Platform Layer*: The cloud data center analyses the information it has collected about global traffic in this tier, develops a plan, and rationally distributes traffic resources. This layer, having the ability to implement connection management, data management, aided autonomous driving, intelligent navigation, path planning, and information security, is the "smart brain" of the IoV.

A blockchain-based vehicle network architecture (Block-VN) for the smart city was presented in [247]. Building innovative distributed transport management systems is made possible by the robust and secure Block-VN architecture. The authors considered how the network of vehicles evolves with paradigms focused on networking and vehicular information. To handle real-time transportation data, Jan et al. [248] created a model for assessing transportation data using Spark and Hadoop. This model/system is separated into four layers: data collection and acquisition, network, data processing, and application. Each layer is built to process and manage data in a structured manner. On the data processing layer, Hadoop and Spark are used to test the data. By utilizing the suggested event and decision mechanism based on *Named Data Networking* [249], the data are made available to a smart community member. The suggested approach was examined using transportation datasets from some reliable sources. The outcomes demonstrate data processing and real-time distribution to citizens in the shortest amount of time. Spark with the Hadoop environment produces findings that are quite accurate. From another viewpoint, Social IoV (SIoV) are a breed of socially aware ephemeral networks [250], where vehicular nodes share/exchange information with different entities and are thus forth comparable with traditional social networks. Kerrache et al. [251] proposed a trust-aware communication

architecture for social IoV (TACASHI), which offers a trust-aware social in-vehicle and inter-vehicle communication architecture for SIVs.

5.7. Architectures for Smart Rural Areas/Smart Villages

The smart village paradigm digitizes various aspects of rural activities using IoT technologies. In the countryside, a variety of activities are carried out, including smart agriculture, waste management, irrigation management, livestock management, smart energy, smart healthcare, and smart education. A smart village or smart rural area can enable real-time data analytics and automate decision-making for local villagers regarding healthcare, agriculture, environment, transportation, and energy. It differs from a smart city as there are key differences (e.g., low cost, infrastructure, and sustainability) between urban and rural environments [252]. To realize the smart village goal, The European Commission (2017) [253] launched an action plan, in which it proposed to interfere ICTs in villages. Cambra-Fierro and Pérez [254] addressed the meaning of “smart” in rural contexts as well as its link with sustainability. The European Commission-funded Smart Rural 21 initiative [255], which has the ultimate goal of encouraging and motivating communities to create and execute smart village methods and tactics throughout Europe as a tool for rural development, serving as the authors’ primary source. IEEE Smart Village [256] also supports the world’s energy-impoveryed communities by providing a complete solution combining renewable energy, community-based education, and entrepreneurial opportunities.

Malik et al. [257] discussed the implementation details of smart villages with different technologies. They concluded that digitization is only possible if a reliable and robust network and communication infrastructure are installed in the village environment. Shrestha and Drozdenko [258] proposed a Smart Rural framework to mitigate the effects of climate change using IoT and the Cloud, building a prototype on the Louisiana Tech University campus. Their framework is an energy-efficient monitoring system for observing the environmental conditions that affect agricultural production and human health. It consists of the following subsystems: Wireless Sensor Nodes, Fog Server, Cloud Services, and a Web Dashboard. The dashboard converts raw sensor data into meaningful information from which public officials and residents can adapt to or frustrate the effects of climate change. Monzon Baeza and Alvarez Marban [259] proposed a flexible and scalable Smart Rural system for gathering and processing IoT data from remote rural areas with no traditional communication coverage as a handicap. The authors offered an architecture structured in separate segments using IoT, 5G, Cloud, and High-Altitude Platform Station (HAPS). Their proposal is applied to the rural environment to thus cover all the needs of the system in the collection of IoT data from these remote rural areas, its coverage by space vehicles, and its processing and storage through 5G terrestrial networks and cloud services. Their proposal includes the deployment of IoT sensors and the development of Amazon Web Services. Conversely, the part of the space segment, considered by HAPS, has been simulated for different space channels. This method provides a complete and automated smart rural system that allows access to these IoT data from remote rural areas through the Internet. To provide secure services close to end-devices, Aljuhani et al. [260] explored the integration of a Distributed Fog Computing (DFC) network architecture with IoT in improving security and privacy solutions for villagers and consumer electronic (CE) devices. As a case study, the authors designed and evaluated the performance of an Intrusion Detection System (IDS) in a DFC-based smart village environment. Moreover, they discussed open security issues and challenges regarding Fog-to-Things enabled smart villages. Rohan et al. [261] proposed a collaborative edge-computing architecture considering the resource constraints in a smart village. The authors illustrated the concept of collaborative edge computing as applicable to reduce cost and better manage the existing infrastructural facilities. Collaboration occurs between the multiple IoT edge devices (e.g., the edge data centers or edge routers) for data processing and storage. For example, in times of high computational load demand, one village’s edge devices can collaborate with another village’s edge devices.

6. Summary

- Various SCAs have different network requirements such as bandwidth, delay tolerance, power consumption, reliability, wireless connectivity, mobility, security, and privacy. Therefore, they need different protocols at the OSI-RM layers. The network architectures for IoT are heterogeneous and include various network technologies such as WiFi, WSNs, Mesh Wireless Networks (WMNs), Vehicular Networks, and Mobile Communication Networks (MCNs) (5G/LTE/4G/3G). The standards adopted in these architectures must allow interoperability, while cross-layer design-based recommendations for power consumption and congestion control are well-suited proposals.
- State-of-the-art generic network architectures for smart cities adopt the SDN paradigm and are based on FogC to reduce latency and increase the efficiency of provided services.
- Fog and ClCom will be used in smart grid communication system architecture in the future to fulfill QoS needs. Such architecture will additionally feature communication methods that can lessen QoS issues like latency, security, and spectrum efficiency. The CR technology will be an indispensable part of this architecture as this technology can quickly reconfigure the operating parameters of the SG communication system to the changing requirements through cognition.
- By extracting usable data from both the physical and network data space, it is possible to increase network security and transportation safety in IoVs. Future IoV architectures will become cognitive. These architectures will include cognitive data engines that will conduct cognition of user tasks by the use of data collected, e.g., driving behavior model analysis, emotion analysis, and road condition investigation.
- The networking performance of SDN is better than the customary networking of smart buildings (SB). However, as Younus et al. [190] state, it also has been facing some challenges such as network management in terms of maintenance, east–west interface, southbound interface, traffic management, energy, ML-based SDN networking for SB, and the network resources issue of SB SDN-based networking.

7. Open Research Issues

—*Network slicing management is required:* IoT services such as smart transportation and smart energy have diversified requirements. To accommodate diverse IoT services, the network slicing paradigm is suggested because it enables multiple independent logical networks running on the same physical network infrastructure. Wu et al. [9] presented an architecture for intelligent network slicing management for the Industrial IoT (IIoT) focusing on three IIoT services (smart transportation, smart energy, and smart factory). The authors also provided a comprehensive survey on intelligent network slicing management in this field.

—*NFV Implementation in the SDN-IoT Environment:* The ETSI Industry Specification Group proposed NFV to virtualize the network functions that were before performed by some proprietary dedicated. NFV allows for the flexible provisioning of software-based network functionalities on top of an appropriately shared physical infrastructure by separating the network functions from the underlying hardware appliances [262]. Utilizing inexpensive commodity servers, it solves the issue of operating costs associated with administering and controlling this closed and proprietary equipment. When SDN is used in conjunction with NFV (the software-defined NFV architecture), it can overcome the difficulties associated with intelligent service orchestration and dynamic resource management [263]. SDN can dynamically establish a virtual service environment through NFV. As a result, the need for specialized hardware and labor-intensive effort to fulfill a new service request is avoided. In conjunction with the use of SDN, NFV also allows real-time and dynamic function provisioning along with flexible traffic forwarding. The SDN-IoT network may be improved and secured with NFV. It enables the software-based deployment of network devices as virtualized components. Throughput is increased because of NFV integration in the SDN-IoT network, which enhances network performance. To this end, Sinh et al. [264] proposed a practical model for hosting IoT services and building

SDN controller applications to show that SDN/NFV can effectively apply to IoT services. Recently, Mukherjee et al. [265] proposed an SDN-based distributed IoT network with NFV implementation for smart cities.

—*Cognitive IoT network architecture for smart cities:* CR technology can address the bandwidth needs of IoT applications [266]. IoT devices can be enabled with cognitive functionalities, including spectrum sensing, dynamic spectrum accessing, circumstantial perceiving, and self-learning. Many SCAs and services can be based on CR technology because it can do dynamic sensing and cognition of the surrounding environment. For example, in smart grid applications, cognitive IoT can achieve the objective of enabling users to know their energy consumption at any time and anywhere [267]. In smart home applications, cognitive-radio-equipped sensors can handle potential heterogeneous network interference [268]. At the same time, cognitive IoT can help with smoother real-time monitoring over longer distances in the healthcare industry without worrying about spectrum availability [269]. The complete utilization of cognitive radio technology in IoT demands extensive research in spectrum optimization, standardization, hardware design, privacy protection, heterogeneous network fusion, scalability and flexibility problems, etc. [270]. For this reason, many CIoT-based smart city network architectures must be proposed to solve such problems. In this regard, Park et al. [271] suggested a CIoT-based smart city network architecture that outlines how data collected from SCAs may be analyzed using the CogC paradigm and manage the scalability and flexibility challenges.

—*Challenges in IoT communication through TCP/IP suite:* Unfortunately, many Access Points (APs) can utilize identical WiFi channels in overlapping regions, leading to interference problems that can significantly impair TCP performance over WiFi [272]. Now, many APs can provide support for wireless access to numerous users in a WiFi network with the DownLink multi-user MIMO (DL MU-MIMO) functionality. DL MU-MIMO is a PHY layer technology (included with IEEE 802.11ac standard [273]) that increases the capacity of WLANs by simultaneously broadcasting data streams to several stations. As a result, it is possible to achieve greater data rates that are equal to the number of antennas on APs. Thus, several stations are served at once. Pokhrel and Singh [131] stressed the employment of CR and Federated Learning (FL) methods with many APs to improve the Compound TCP's performance in wide-area Industry 4.0 WiFi networks. An FL method can accelerate the learning processes of the transport protocols such as Compound TCP. In FL, training data are dispersed across a large number of clients, each having unreliable and comparatively slow network connections, with the aim of developing a high-quality centralized model. The authors of [131] insisted on using these specialized strategies to coordinate numerous APs with regard to losses caused by unique wireless channel characteristics and WiFi downloading and uploading dynamics. Through the use of FL and CR approaches in dual AP settings, it is now possible to improve the Layer-4 performances of TCP versions. Another study [274] assumed TCP Cubic [275] as the Layer-4 protocol and considered the FL approach for IoVs. The authors of [276] developed a framework for exploiting the FL technique, which enhances the efficiency and privacy protection for the case of IoVs.

—*Digital Twins for Smart Processes:* A virtual depiction of resources, personnel, procedures, systems, devices, and locations is referred to as a *digital twin*. Digital twin technology can be used to duplicate a variety of objects, including humans, IoT devices, aircraft engines, and vehicles. A digital twin of the original vehicle is created, for instance, when an automobile business creates a virtual representation or digital duplicate (copy) of a car model. If a manufacturer creates a virtual representation of its manufacturing process, the replicated process is a digital twin of the physical process. A digital twin is a profile of the actual process or physical object's past and present state. In this virtual graphic, the dynamics and features of an IoT device's life and operation are depicted. The digital twin can offer the location, state, and/or status of physical assets in real-time due to continual learning and advancements. This fusion of the real and digital worlds enables organizations to monitor systems, set strategies, and anticipate problems before they occur. Digital twins are created using digital twin technology, which integrates network infrastructure graphs,

AI, software analytics, and the IoT. Through digital twins, the idea of the smart city is demonstrated. This technology can efficiently administer the city, from urban planning to the optimization of land use. Digital twins make it possible to simulate plans before putting them into action in the real world, revealing issues before they materialize. If a digital twin is in place, government organizations can only fully assess what might be achieved with the data to better citizens' lives, offer economic opportunity, and establish a more cohesive community. Although the idea is currently novel, it is expected to catch on in the next few years [277].

—*The 6G Network for Futuristic Smart Cities:* A futuristic smart city is a dense and AI-centric city because massive device connectivity with vast data traffic is estimated in the future. In such cities, the concept of IoT will be converted to the concept of Internet of Everything (IoE). Networks of futuristic smart cities should have a huge bandwidth, low latency, and AI integration. Such networks should also provide ubiquity, high QoS, and on-demand content for thousands of interconnected devices. The 6G network [278] is the problem-solving network of futuristic cities, with huge bandwidth and low latency. It is under development for wireless communications technologies supporting cellular data networks. Like its predecessors, 6G networks will probably be broadband cellular networks, in which the service area is divided into small geographical areas (cells). It is expected that 6G will be supported by existing 5G infrastructures such as SDN, NFV, and network slicing, together with new infrastructure. The network requirements of 6G are as follows [278]: (1) ultra-fast data rates as high as 1 Tbps; (2) ultra-low latency of less than 1 ms; (3) increased mobility and coverage; (4) flexible and efficient connection of trillion level objects; (5) peak spectral efficiency of 60 b/s/Hz; (6) very high system reliability; and (7) improved network security [279]. However, the main problem of 6G is that transmitting at a higher frequency spectrum is prone to high path loss, making the distance for transmission limited [280]. The expected 6G of the radio access network is based on terahertz (THz) waves with the capability of carrying up to one terabit per second (Tbps). THz waves have the capability of carrying a large amount of data, but these waves have numerous drawbacks, such as short-range and atmospheric attenuation. Hence, these drawbacks can introduce complications and hinder the performance of the 6G network. Therefore, such complications of THz waves must be considered, and efficient AI-centric multilayer physical network architectures of 6G must be proposed for futuristic smart cities. Farooq et al. [280] considered the expectations from a network of futuristic smart cities and the problems of THz waves and proposed a conceptual terrestrial network (TN) architecture for 6G. The nested Bee Hive [280] is a scalable multilayer architecture designed to meet the needs of futuristic smart cities. It provides an on-ground cloud network that helps smart devices to run AI applications partially on their own and the rest on the cloud. Furthermore, the distributed and edge computing-oriented infrastructure of Bee Hive provides security and reduces traffic load on the upper layer of the network. Undoubtedly, pervasive AI is the main enabling technology in 6G, while some forms of AI are realized as part of 5G. Many successful examples of using AI on wireless communications have been proposed, from physical layer designs (e.g., channel estimation and precoding), to network resource allocation (e.g., traffic control and cache storage management), to security and authentication, to dynamic cell and topology formation and management, to fault prediction and detection, etc. However, DL-based solutions require high computational complexity, which might not fit in current mobile phones [281]. Apart from the complexity, Artificial Neural Network (ANN)-based RL algorithms must be carefully designed to decrease the computational resources required on these devices [282]. Quantum communication [283] offers a promising approach to avoiding the challenge of limited computational resources and energy efficiency. Applying Artificial Neural Networks in IoT also comes with the trade-off challenge between accuracy and computational/energy requirements [282]. Tariq et al. [284] studied some of the above issues and envisioned 6G to facilitate futuristic smart cities with pervasive autonomous systems. Apart from pervasive AI, Imoize et al. [285] discussed other important enabling technologies of 6G and their challenges. These enabling technologies are as follows:

- Reconfigurable Intelligent Surfaces (RISs) [286] that reflect signals and help in places where maintaining Line of Sight (LoS) is difficult. RISs will be mainly deployed on doors, windows, and buildings.
- Cell-Free Massive MIMO: The massive MIMO technology is introduced in 5G with a more dense network of access points (APs), and this is further developed in 6G to include a network with no cells (cell-free) [287]. Cell-Free Massive MIMO improves spectral efficiency in communication networks, but there are some health risks associated with such a dense network of APs.
- CubeSat communication or the Internet of Space Things [288]. A CubeSat (or U-class spacecraft) is a miniaturized spacecraft with sizes that are multiples of U, up to 6U, and U being $10 \times 10 \times 10$ cm cubic units.
- UAVs/satellite communication.
- Terahertz communication and Optical Wireless Technology [289].
- Blockchain technology [290] and quantum communication [283].

The development of futuristic smart cities keeps up with the development of energy-efficient 6G communication. Kamruzzaman [291] presented the key trends in the IoT for energy-efficient 6G wireless communication in smart cities. He argues that the application of IoT devices to 6G in smart cities will provide a 100 Gbps data rate, <0.1 ms latency rate, up to 1000 km/h mobility rate, 100 bps/Hz spectral efficiency, and 1000 GHz frequency. This will resolve the issues of energy inefficiency and other concerns in conventional communication networks. Moreover, the use of energy-efficient 6G in smart cities via IoT devices probably will solve various problems that are encountered by existing smart city systems. In futuristic smart cities, residents will use the innovative 6G brain-computer interface (BCI) technology [292] for a multi-sense experience. BCI is based on the signals and information that monitor and control machines using sensible wearable headsets and devices. It uses human consciousness more than external sources for better interaction. As humans have five senses (sight, hearing, touch, smell, and taste), BCI comprises five datasets, comprising features of human senses that are used for human interaction with the machine [292].

8. Conclusions

Utilizing resources efficiently, reducing operating expenses, and enhancing city dwellers' quality of life are the objectives of the smart city paradigm. This goal is obtained by combining various technologies including IoT, WSNs, CPS, ClCom, FoC, big data analytics, and robots. For this model, the effective networking and communication between the many components required to enable various SCAs are crucial for achieving its objectives. The ever-increasing need for networking leads to many elastic and manageable platforms for various SCAs including smart grid, smart buildings, smart home, smart water, and smart transportation systems. The networking needs of the key SCAs were examined in this research, and the appropriate protocols that can be applied at different system levels have been identified. Additionally, we provided examples of networking protocols and smart grid, intelligent building, smart residence, and smart transportation system architectures. We concentrated on key criteria for a variety of networking designs, such as energy savings, routing, security, dependability, mobility, and support for heterogeneous networks. In addition, we presented open research issues.

This survey can assist researchers to recognize research gaps/problems working in the networking architectures for smart cities, and it provides an overview of available protocols and architectures for SCAs.

Author Contributions: Conceptualization, D.K.; methodology, D.K. and V.K.S.; analysis and investigation, D.K. and V.K.S.; draft preparation, D.K., V.K.S. and T.P.; supervision, A.K. All authors have read and agreed to the published version of the manuscript.

Funding: This research work was supported by the research project CRISIS, “Competences for Resilient Smart Cities’ Staff” (Project No.: 2021-1-EL01-KA220-HED-000032257, Erasmus+ KA2—Partnerships for Cooperation).

Data Availability Statement: Not applicable.

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

Abbreviations

The following abbreviations are used in this manuscript:

AMI	Automatic Metering Infrastructure
AMQP	Advanced Message Queuing Protocol
AODV	Ad-Hoc On-Demand Distance Vector
API	Application Programming Interface
AQMS	Indoor Air Quality Monitoring System
BLE	Bluetooth Low Energy
CICom	Cloud Computing
CoAP	Constrained Application Protocol
CPS	Cyber-Physical System
CR	Cognitive Radio
DDS	Data Distribution Service
DERs	Distributed Energy Resources
DL	Deep Learning
D2D	Device-to-Device communication
EPS	Electric Power System
ETSI	European Telecommunications Standards Institute
FoC	Fog Computing
HTTP	Hypertext Transfer Protocol
HVAC	Heating, Ventilating, and Air-Conditioning
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IoT	Internet of Things
IoV	Internet of Vehicles
IPv6	Internet Protocol version 6
ISP	Internet Service Provider
LAN	Local Area Network
LoRA	Long Range (a spread spectrum modulation technique)
LPWAN	Low-Power Wide Area Network
LTE	Long-Term Evolution
MAC	Medium Access Control
MLB	Multipath Load-Balancing (routing)
MQTT	Message Queuing Telemetry Transport
M2M	Machine-to-Machine
NFV	Network Function Virtualization
OSI-RM	Open Systems Interconnection—Reference Model
PAN	Personal Area Network
PEVs	Plug-in Electric Vehicles
PHY	Physical layer
QoE	Quality of Experience
QoS	Quality of Service
REST	Representational State Transfer protocol
RFID	Radio-Frequency Identification
RPL	Routing Protocol for Low-Power and Lossy Networks
SBA	Smart Building Architecture
SCA	Smart City Application
SCADA	Supervisory Control and Data Acquisition (system)
SDN	Software Defined Networking
SG	Smart Grid

SWS	Smart Water System
TCP	Transmission Control Protocol
UAV	Unmanned Aerial Vehicle
UDP	User Datagram Protocol
VANET	Vehicular Ad-hoc Network
WAN	Wide Area Network
WSN	Wireless Sensor Network
XML	Extensible Markup Language
XMPP	Extensible Messaging and Presence Protocol
5G	Fifth Generation
6G	Sixth Generation
6LoWPAN	IPv6 over Low-Power Wireless Personal Area Network

References

1. Achmad, K.A.; Nugroho, L.E.; Djunaedi, A. Smart city model: A literature review. In Proceedings of the 2018 10th International Conference on Information Technology and Electrical Engineering (ICITEE), Bali, Indonesia, 24–26 July 2018; pp. 488–493. [[CrossRef](#)]
2. Al-Fuqaha, A.; Guizani, M.; Mohammadi, M.; Aledhari, M.; Ayyash, M. Internet of things: A survey on enabling technologies, protocols, and applications. *IEEE Commun. Surv. Tutor.* **2015**, *17*, 2347–2376. [[CrossRef](#)]
3. Khalifeh, A.; Darabkh, K.A.; Khasawneh, A.M.; Alqaisieh, I.; Salameh, M.; AlAbdala, A.; Alrubaye, S.; Alassaf, A.; Al-HajAli, S.; Al-Wardat, R.; et al. Wireless sensor networks for smart cities: Network design, implementation and performance evaluation. *Electronics* **2021**, *10*, 218. [[CrossRef](#)]
4. Puliafito, A.; Tricomi, G.; Zafeiropoulos, A.; Papavassiliou, S. Smart cities of the future as cyber physical systems: Challenges and enabling technologies. *Sensors* **2021**, *21*, 3349. [[CrossRef](#)] [[PubMed](#)]
5. Alam, T. Cloud-based IoT applications and their roles in smart cities. *Smart Cities* **2021**, *4*, 1196–1219. [[CrossRef](#)]
6. Hu, P.; Dhelim, S.; Ning, H.; Qiu, T. Survey on fog computing: Architecture, key technologies, applications and open issues. *J. Netw. Comput. Appl.* **2017**, *98*, 27–42. [[CrossRef](#)]
7. Beigi, N.K.; Partov, B.; Farokhi, S. Real-time cloud robotics in practical smart city applications. In Proceedings of the 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), Montreal, QC, Canada, 8–13 October 2017; pp. 1–5. [[CrossRef](#)]
8. Osman, A.M.S. A novel big data analytics framework for smart cities. *Future Gener. Comput. Syst.* **2019**, *91*, 620–633. [[CrossRef](#)]
9. Wu, Y.; Dai, H.N.; Wang, H.; Xiong, Z.; Guo, S. A survey of intelligent network slicing management for industrial IoT: Integrated approaches for smart transportation, smart energy, and smart factory. *IEEE Commun. Surv. Tutor.* **2022**, *24*, 1175–1211. [[CrossRef](#)]
10. Marinakis, V.; Doukas, H.; Tsapelas, J.; Mouzakitis, S.; Sicilia, Á.; Madrazo, L.; Sgouridis, S. From big data to smart energy services: An application for intelligent energy management. *Future Gener. Comput. Syst.* **2020**, *110*, 572–586. [[CrossRef](#)]
11. Sony, S.; Laventure, S.; Sadhu, A. A literature review of next-generation smart sensing technology in structural health monitoring. *Struct. Control Health Monit.* **2019**, *26*, e2321. [[CrossRef](#)]
12. Lacinák, M.; Ristvej, J. Smart city, safety and security. *Procedia Eng.* **2017**, *192*, 522–527. [[CrossRef](#)]
13. Kitchenham, B. *Procedures for Performing Systematic Reviews*; Technical Report TR/SE-0401; Keele University: Keele, UK, 2004. Available online: <https://www.inf.ufsc.br/~aldo.vw/kitchenham.pdf> (accessed on 10 February 2023).
14. Butt, O.M.; Zulqarnain, M.; Butt, T.M. Recent advancement in smart grid technology: Future prospects in the electrical power network. *Ain Shams Eng. J.* **2021**, *12*, 687–695. [[CrossRef](#)]
15. Jha, A.V.; Appasani, B.; Ghazali, A.N.; Pattanayak, P.; Gurjar, D.S.; Kabalci, E.; Mohanta, D.K. Smart grid cyber-physical systems: Communication technologies, standards and challenges. *Wirel. Netw.* **2021**, *27*, 2595–2613. [[CrossRef](#)]
16. Schmidt, M.; Åhlund, C. Smart buildings as Cyber-Physical Systems: Data-driven predictive control strategies for energy efficiency. *Renew. Sustain. Energy Rev.* **2018**, *90*, 742–756. [[CrossRef](#)]
17. Yurtsever, E.; Lambert, J.; Carballo, A.; Takeda, K. A survey of autonomous driving: Common practices and emerging technologies. *IEEE Access* **2020**, *8*, 58443–58469. [[CrossRef](#)]
18. Mao, T.; Mihăită, A.S.; Chen, F.; Vu, H.L. Boosted genetic algorithm using machine learning for traffic control optimization. *IEEE Trans. Intell. Transp. Syst.* **2022**, *23*, 7112–7141. [[CrossRef](#)]
19. Wang, Z.; Song, H.; Watkins, D.W.; Ong, K.G.; Xue, P.; Yang, Q.; Shi, X. Cyber-physical systems for water sustainability: Challenges and opportunities. *IEEE Commun. Mag.* **2015**, *53*, 216–222. [[CrossRef](#)]
20. Jan, F.; Min-Allah, N.; Düstegör, D. IoT based smart water quality monitoring: Recent techniques, trends and challenges for domestic applications. *Water* **2021**, *13*, 1729. [[CrossRef](#)]
21. Kochhar, A.; Kumar, N. Wireless sensor networks for greenhouses: An end-to-end review. *Comput. Electron. Agric.* **2019**, *163*, 104877. [[CrossRef](#)]
22. Cheng, L.; Wang, T.; Hong, X.; Wang, Z.; Wang, J.; Liu, J. A study on the architecture of manufacturing internet of things. *Int. J. Model. Identif. Control* **2015**, *23*, 8–23. [[CrossRef](#)]

23. Dafflon, B.; Moalla, N.; Ouzrout, Y. The challenges, approaches, and used techniques of CPS for manufacturing in Industry 4.0: A literature review. *Int. J. Adv. Manuf. Technol.* **2021**, *113*, 2395–2412. [CrossRef]
24. Satyanarayanan, M. The emergence of edge computing. *Computer* **2017**, *50*, 30–39. [CrossRef]
25. Chen, M.; Li, W.; Hao, Y.; Qian, Y.; Humar, I. Edge cognitive computing based smart healthcare system. *Future Gener. Comput. Syst.* **2018**, *86*, 403–411. [CrossRef]
26. Javaid, S.; Sufian, A.; Pervaiz, S.; Tanveer, M. Smart traffic management system using Internet of Things. In Proceedings of the 2018 20th International Conference on Advanced Communication Technology (ICACT), Chuncheon, Republic of Korea, 11–14 February 2018; pp. 393–398. [CrossRef]
27. Afrin, T.; Yodo, N. A survey of road traffic congestion measures towards a sustainable and resilient transportation system. *Sustainability* **2020**, *12*, 4660. [CrossRef]
28. Sarrab, M.; Pulparambil, S.; Awadalla, M. Development of an IoT based real-time traffic monitoring system for city governance. *Glob. Transit.* **2020**, *2*, 230–245. [CrossRef]
29. Zeadally, S.; Siddiqui, F.; Baig, Z.; Ibrahim, A. Smart healthcare: Challenges and potential solutions using internet of things (IoT) and big data analytics. *PSU Res. Rev.* **2020**, *4*, 149–168. [CrossRef]
30. Alromaihi, S.; Elmedany, W.; Balakrishna, C. Cyber security challenges of deploying IoT in smart cities for healthcare applications. In Proceedings of the 6th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW), Barcelona, Spain, 6–8 August 2018; pp. 140–145. [CrossRef]
31. Baker, S.B.; Xiang, W.; Atkinson, I. Internet of things for smart healthcare: Technologies, challenges, and opportunities. *IEEE Access* **2017**, *5*, 26521–26544. [CrossRef]
32. Qadri, Y.A.; Nauman, A.; Zikria, Y.B.; Vasilakos, A.V.; Kim, S.W. The future of healthcare internet of things: A survey of emerging technologies. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 1121–1167. [CrossRef]
33. Concas, F.; Mineraud, J.; Lagerspetz, E.; Varjonen, S.; Liu, X.; Puolamäki, K.; Nurmi, P.; Tarkoma, S. Low-cost outdoor air quality monitoring and sensor calibration: A survey and critical analysis. *ACM Trans. Sens. Netw.* **2021**, *17*, 1–44. [CrossRef]
34. Bloomer, M. The Challenges and Complexities of Weather Forecasting. Available online: <https://www.weather.gov/car/weatherforecasting> (accessed on 10 January 2023).
35. Sosunova, I.; Porras, J. IoT-enabled smart waste management systems for smart cities: A systematic review. *IEEE Access* **2022**, *10*, 73326–73363. [CrossRef]
36. Omar, A.; AlMaeeni, S.; Attia, H.; Takruri, M.; Altunaiji, A.; Sanduleanu, M.; Shubair, R.; Ashhab, M.S.; Al Ali, M.; Al Hebsi, G. Smart city: Recent advances in intelligent street lighting systems based on IoT. *J. Sens.* **2022**, *2022*, 5249187. [CrossRef]
37. Zanella, A.; Bui, N.; Castellani, A.; Vangelista, L.; Zorzi, M. Internet of things for smart cities. *IEEE Internet Things J.* **2014**, *1*, 22–32. [CrossRef]
38. Gharaibeh, A.; Salahuddin, M.A.; Hussini, S.J.; Khreishah, A.; Khalil, I.; Guizani, M.; Al-Fuqaha, A. Smart cities: A survey on data management, security, and enabling technologies. *IEEE Commun. Surv. Tutor.* **2017**, *19*, 2456–2501. [CrossRef]
39. Fernandes, E.; Jung, J.; Prakash, A. Security analysis of emerging smart home applications. In Proceedings of the 2016 IEEE Symposium on Security and Privacy, San Jose, CA, USA, 22–26 May 2016; pp. 636–654. [CrossRef]
40. Vault7-Home. Available online: <https://wikileaks.org/ciav7p1/index.html> (accessed on 10 January 2023).
41. El-Hajj, M.; Fadlallah, A.; Chamoun, M.; Serhrouchni, A. A survey of internet of things (IoT) authentication schemes. *Sensors* **2019**, *19*, 1141. [CrossRef] [PubMed]
42. Bari, A.; Jiang, J.; Saad, W.; Jaekel, A. Challenges in the smart grid applications: An overview. *Int. J. Distrib. Sens. Netw.* **2014**, *10*, 974682. [CrossRef]
43. Wang, W.; Xu, Y.; Khanna, M. A survey on the communication architectures in smart grid. *Comput. Netw.* **2011**, *55*, 3604–3629. [CrossRef]
44. Khan, R.H.; Khan, J.Y. A comprehensive review of the application characteristics and traffic requirements of a smart grid communications network. *Comput. Netw.* **2013**, *57*, 825–845. [CrossRef]
45. Kuzlu, M.; Pipattanasomporn, M.; Rahman, S. Communication network requirements for major smart grid applications in HAN, NAN and WAN. *Comput. Netw.* **2014**, *67*, 74–88. [CrossRef]
46. Abdullah, A.A.; Hassan, T.M. Smart grid (SG) properties and challenges: An overview. *Discov. Energy* **2022**, *2*, 8. [CrossRef]
47. Gao, J.; Xiao, Y.; Liu, J.; Liang, W.; Chen, C.P. A survey of communication/networking in smart grids. *Future Gener. Comput. Syst.* **2012**, *28*, 391–404. [CrossRef]
48. Kansal, P.; Bose, A. Bandwidth and latency requirements for smart transmission grid applications. *IEEE Trans. Smart Grid* **2012**, *3*, 1344–1352. [CrossRef]
49. Jawhar, I.; Mohamed, N.; Al-Jaroodi, J. Networking architectures and protocols for smart city systems. *J. Internet Serv. Appl.* **2018**, *9*, 26. [CrossRef]
50. Shoaib, N.; Shamsi, J.A. Understanding network requirements for smart city applications: Challenges and solutions. *IT Prof.* **2019**, *21*, 33–40. [CrossRef]
51. Sesia, S.; Toufik, I.; Baker, M. *LTE—the UMTS Long Term Evolution: From Theory to Practice*; John Wiley & Sons: Hoboken, NJ, USA, 2011.
52. Chin, W.H.; Fan, Z.; Haines, R. Emerging technologies and research challenges for 5G wireless networks. *IEEE Wirel. Commun.* **2014**, *21*, 106–112. [CrossRef]

53. Ramya, C.M.; Shanmugaraj, M.; Prabakaran, R. Study on ZigBee technology. In Proceedings of the 3rd International Conference on Electronics Computer Technology, Kanyakumari, India, 8–10 April 2011; Volume 6, pp. 297–301. [CrossRef]
54. Atat, R.; Liu, L.; Chen, H.; Wu, J.; Li, H.; Yi, Y. Enabling cyber-physical communication in 5G cellular networks: Challenges, spatial spectrum sensing, and cyber-security. *IET Cyber-Phys. Syst. Theory Appl.* **2017**, *2*, 49–54. [CrossRef]
55. Khorov, E.; Lyakhov, A.; Krotov, A.; Guschin, A. A survey on IEEE 802.11ah: An enabling networking technology for smart cities. *Comput. Commun.* **2015**, *58*, 53–69. [CrossRef]
56. Kim, D.Y.; Jung, M. Data transmission and network architecture in long range low power sensor networks for IoT. *Wirel. Pers. Commun.* **2017**, *93*, 119–129. [CrossRef]
57. Ratasuk, R.; Vejlgaard, B.; Mangalvedhe, N.; Ghosh, A. NB-IoT system for M2M communication. In Proceedings of the 2016 IEEE Wireless Communications and Networking Conference, Doha, Qatar, 3–6 April 2016; pp. 1–5. [CrossRef]
58. Perera, C.; Qin, Y.; Estrella, J.C.; Reiff-Marganiec, S.; Vasilakos, A.V. Fog computing for sustainable smart cities: A survey. *ACM Comput. Surv.* **2017**, *50*, 1–43. [CrossRef]
59. Alvi, S.A.; Afzal, B.; Shah, G.A.; Atzori, L.; Mahmood, W. Internet of multimedia things: Vision and challenges. *Ad Hoc Netw.* **2015**, *33*, 87–111. [CrossRef]
60. Avelar, E.; Marques, L.; dos Passos, D.; Macedo, R.; Dias, K.; Nogueira, M. Interoperability issues on heterogeneous wireless communication for smart cities. *Comput. Commun.* **2015**, *58*, 4–15. [CrossRef]
61. Cohen, E.G.; Ho, D.; Mohanty, B.P.; Rajkotia, P.R.; Berger, L.T.; Schwager, A.; Schneider, D.M. IEEE 1905.1: Convergent digital home networking. In *MIMO Power Line Communications: Narrow and Broadband Standards, EMC, and Advanced Processing*; CRC: Boca Raton, FL, USA, 2014.
62. Del Esposte, A.D.M.; Santana, E.F.; Kanashiro, L.; Costa, F.M.; Braghetto, K.R.; Lago, N.; Kon, F. Design and evaluation of a scalable smart city software platform with large-scale simulations. *Future Gener. Comput. Syst.* **2019**, *93*, 427–441. [CrossRef]
63. Kanellopoulos, D.; Sharma, V.K. Dynamic load balancing techniques in the IoT: A review. *Symmetry* **2022**, *14*, 2554. [CrossRef]
64. Liu, Q.; Gu, J.; Yang, J.; Li, Y.; Sha, D.; Xu, M.; Shams, I.; Yu, M.; Yang, C. Cloud, edge, and mobile computing for smart cities. In *Urban Informatics*; The Urban Book Series; Shi, W., Goodchild, M.F., Batty, M., Kwan, M.P., Zhang, A., Eds.; Springer: Singapore, 2021. [CrossRef]
65. da Silva, T.P.; Batista, T.; Lopes, F.; Neto, A.R.; Delicato, F.C.; Pires, P.F.; da Rocha, A.R. Fog computing platforms for smart city applications-A survey. *ACM Trans. Internet Technol.* **2022**, *22*, 1–32. [CrossRef]
66. Mouradian, C.; Naboulsi, D.; Yangui, S.; Glitho, R.H.; Morrow, M.J.; Polakos, P.A. A comprehensive survey on fog computing: State-of-the-art and research challenges. *IEEE Commun. Surv. Tutor.* **2017**, *20*, 416–464. [CrossRef]
67. Coady, Y.; Hohlfeld, O.; Kempf, J.; McGeer, R.; Schmid, S. Distributed cloud computing: Applications, status quo, and challenges. *ACM SIGCOMM Comput. Commun. Rev.* **2015**, *45*, 38–43. [CrossRef]
68. Ksentini, A.; Jebalia, M.; Tabbane, S. IoT/cloud-enabled smart services: A review on QoS requirements in fog environment and a proposed approach based on priority classification technique. *Int. J. Commun. Syst.* **2021**, *34*, e4269. [CrossRef]
69. OpenFog Consortium Architecture Working Group. OpenFog Reference Architecture for Fog Computing. 2017. Available online: https://www.iiconsortium.org/pdf/OpenFog_Reference_Architecture_2_09_17.pdf (accessed on 10 January 2023).
70. Theoleyre, F.; Watteyne, T.; Bianchi, G.; Tuna, G.; Gungor, V.C.; Pang, A.C. Networking and communications for smart cities special issue editorial. *Comput. Commun.* **2015**, *58*, 1–3. [CrossRef]
71. Conti, M.; Giordano, S. Mobile ad hoc networking: Milestones, challenges, and new research directions. *IEEE Commun. Mag.* **2014**, *52*, 85–96. [CrossRef]
72. Winter, T.; Thubert, P.; Brandt, A.; Hui, J.; Kelsey, R.; Levis, P.; Pister, K.; Struik, R.; Vasseur, J.P.; Alexander, R. RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks. RFC 6550. 2012. Available online: <https://www.rfc-editor.org/rfc/rfc6550.html> (accessed on 1 February 2023).
73. Kushalnagar, N.; Montenegro, G.; Schumacher, C. IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals. RFC 4919. 2007. Available online: <https://www.rfc-editor.org/rfc/rfc4919> (accessed on 1 February 2023).
74. Soltanmohammadi, E.; Ghavami, K.; Naraghi-Pour, M. A survey of traffic issues in machine-to-machine communications over LTE. *IEEE Internet Things J.* **2016**, *3*, 865–884. [CrossRef]
75. Velliangiri, S.; NG, B.A.; Baik, N.K. Detection of DoS attacks in smart city networks with feature distance maps: A statistical approach. *IEEE Internet Things J.* **2023**; Early Access. [CrossRef]
76. Hassan, W.H. Current research on Internet of Things (IoT) security: A survey. *Comput. Netw.* **2019**, *148*, 283–294. [CrossRef]
77. Hammi, M.T.; Hammi, B.; Bellot, P.; Serhrouchni, A. Bubbles of Trust: A decentralized blockchain-based authentication system for IoT. *Comput. Secur.* **2018**, *78*, 126–142. [CrossRef]
78. Qu, C.; Tao, M.; Zhang, J.; Hong, X.; Yuan, R. Blockchain based credibility verification method for IoT entities. *Secur. Commun. Netw.* **2018**, *2018*, 7817614. [CrossRef]
79. Erhan, L.; Ndubuaku, M.; Di Mauro, M.; Song, W.; Chen, M.; Fortino, G.; Bagdasar, O.; Liotta, A. Smart anomaly detection in sensor systems: A multi-perspective review. *Inf. Fusion* **2021**, *67*, 64–79. [CrossRef]
80. Ullah, Z.; Al-Turjman, F.; Mostarda, L.; Gagliardi, R. Applications of artificial intelligence and machine learning in smart cities. *Comp. Commun.* **2020**, *154*, 313–323. [CrossRef]

81. Ahmed, S.T.; Kumar, V.; Kim, J. AIoTel: eHealth Augmented Intelligence based Telemedicine Resource Recommendation Framework for IoT devices in Smart cities. *IEEE Internet Things J.* **2023**; *Early Access*. [CrossRef]
82. Heidari, A.; Navimipour, N.J.; Unal, M. Applications of ML/DL in the management of smart cities and societies based on new trends in information technologies: A systematic literature review. *Sustain. Cities Soc.* **2022**, *85*, 104089. [CrossRef]
83. Syed, A.S.; Sierra-Sosa, D.; Kumar, A.; Elmaghraby, A. IoT in smart cities: A survey of technologies, practices and challenges. *Smart Cities* **2021**, *4*, 429–475. [CrossRef]
84. Yaqoob, I.; Hashem, I.A.T.; Mehmood, Y.; Gani, A.; Mokhtar, S.; Guizani, S. Enabling communication technologies for smart cities. *IEEE Commun. Mag.* **2017**, *55*, 112–120. [CrossRef]
85. Fernandes, R.F.; Fonseca, C.C.; Brandão, D.; Ferrari, P.; Flammini, A.; Vezzoli, A. Flexible Wireless Sensor Network for smart lighting applications. In Proceedings of the 2014 IEEE International Instrumentation and Measurement Technology Conference (I2MTC) Proceedings, Montevideo, Uruguay, 12–15 May 2014; pp. 434–439. [CrossRef]
86. Gupta, A.; Jha, R.K. A survey of 5G network: Architecture and emerging technologies. *IEEE Access* **2015**, *3*, 1206–1232. [CrossRef]
87. Yang, C.; Liang, P.; Fu, L.; Cui, G.; Huang, F.; Teng, F.; Bangash, Y.A. Using 5G in smart cities: A systematic mapping study. *Intell. Syst. Appl.* **2022**, *14*, 200065. [CrossRef]
88. Gungor, V.C.; Sahin, D.; Kocak, T.; Ergut, S.; Buccella, C.; Cecati, C.; Hancke, G.P. Smart grid technologies: Communication technologies and standards. *IEEE Trans. Ind. Inform.* **2011**, *7*, 529–539. [CrossRef]
89. García-García, L.; Jiménez, J.M.; Abdullah, M.T.A.; Lloret, J. Wireless technologies for IoT in smart cities. *Netw. Protoc. Algorithms* **2018**, *10*, 23–64. [CrossRef]
90. Bettstetter, C.; Vogel, H.J.; Eberspacher, J. GSM phase 2+ general packet radio service GPRS: Architecture, protocols, and air interface. *IEEE Commun. Surv.* **1999**, *2*, 2–14. [CrossRef]
91. Dahlman, E.; Parkvall, S.; Skold, J. *4G: LTE/LTE-Advanced for Mobile Broadband*; Academic Press: New York, NY, USA, 2013.
92. Jung, W.; Kwon, Y. Differences between LTE and 3G service customers: Business and policy implications. *Telemat. Inform.* **2015**, *32*, 667–680. [CrossRef]
93. Rinaldi, F.; Raschella, A.; Pizzi, S. 5G NR system design: A concise survey of key features and capabilities. *Wirel. Netw.* **2021**, *27*, 5173–5188. [CrossRef]
94. Zaidi, A.A.; Baldemair, R.; Tullberg, H.; Björkegren, H.; Sundstrom, L.; Medbo, J.; Kilinc, C.; Da Silva, I. Waveform and numerology to support 5G services and requirements. *IEEE Commun. Magaz.* **2016**, *54*, 90–98. [CrossRef]
95. Perez-Costa, X.; Camps-Mur, D. IEEE 802.11 E QoS and power saving features overview and analysis of combined performance. *IEEE Wirel. Commun.* **2010**, *17*, 88–96. [CrossRef]
96. Sun, W.; Choi, M.; Choi, S. IEEE 802.11ah: A long range 802.11 WLAN at sub 1 GHz. *J. ICT Stand.* **2013**, *1*, 83–108. [CrossRef]
97. Mozaffarihrar, E.; Theoleyre, F.; Menth, M. A survey of Wi-Fi 6: Technologies, advances, and challenges. *Future Internet* **2022**, *14*, 293. [CrossRef]
98. Khajenasiri, I.; Estebsari, A.; Verhelst, M.; Gielen, G. A review on Internet of Things solutions for intelligent energy control in buildings for smart city applications. *Energy Procedia* **2017**, *111*, 770–779. [CrossRef]
99. Cerruela García, G.; Luque Ruiz, I.; Gómez-Nieto, M.Á. State of the art, trends and future of bluetooth low energy, near field communication and visible light communication in the development of smart cities. *Sensors* **2016**, *16*, 1968. [CrossRef]
100. Bluetooth®Wireless Technology. Available online: <https://www.bluetooth.com/learn-about-bluetooth/tech-overview/> (accessed on 22 January 2023).
101. Faragher, R.; Harle, R. Location fingerprinting with bluetooth low energy beacons. *IEEE JSAC* **2015**, *33*, 2418–2428. [CrossRef]
102. Miorandi, D.; Zanella, A.; Pierobon, G. Performance evaluation of Bluetooth polling schemes: An analytical approach. *Mob. Netw. Appl.* **2004**, *9*, 6372. [CrossRef]
103. Nikoukar, A.; Raza, S.; Poole, A.; Güneş, M.; Dezfouli, B. Low-power wireless for the internet of things: Standards and applications. *IEEE Access* **2018**, *6*, 67893–67926. [CrossRef]
104. Catherwood, P.A.; Steele, D.; Little, M.; Mccomb, S.; McLaughlin, J. A community-based IoT personalized wireless healthcare solution trial. *IEEE J. Transl. Eng. Health Med.* **2018**, *6*, 1–13. [CrossRef]
105. Sharma, V.; You, I.; Pau, G.; Collotta, M.; Lim, J.D.; Kim, J.N. LoRaWAN-based energy-efficient surveillance by drones for intelligent transportation systems. *Energies* **2018**, *11*, 573. [CrossRef]
106. Jawad, H.M.; Nordin, R.; Gharghan, S.K.; Jawad, A.M.; Ismail, M. Energy-efficient wireless sensor networks for precision agriculture: A review. *Sensors* **2017**, *17*, 1781. [CrossRef] [PubMed]
107. Podevijn, N.; Plets, D.; Trogh, J.; Martens, L.; Suanet, P.; Hendrikse, K.; Joseph, W. TDoA-based outdoor positioning with tracking algorithm in a public LoRa network. *Wirel. Commun. Mob. Comput.* **2018**, *2018*, 1864209. [CrossRef]
108. de Castro Tomé, M.; Nardelli, P.H.; Alves, H. Long-range low-power wireless networks and sampling strategies in electricity metering. *IEEE Trans. Ind. Electron.* **2018**, *66*, 1629–1637. [CrossRef]
109. Haxhibeqiri, J.; De Poorter, E.; Moerman, I.; Hoebelke, J. A survey of LoRaWAN for IoT: From technology to application. *Sensors* **2018**, *18*, 3995. [CrossRef]
110. Adelantado, F.; Vilajosana, X.; Tuset-Peiro, P.; Martinez, B.; Melia-Segui, J.; Watteyne, T. Understanding the limits of LoRaWAN. *IEEE Commun. Mag.* **2017**, *55*, 34–40. [CrossRef]
111. IEEE Std. 802.16-2004; IEEE Standard for Local and Metropolitan Area Networks. Part 16: Air Interface for Fixed Broadband Wireless Access Systems. IEEE: Piscataway, NJ, USA, 2004.

112. IEEE Std. 802.16e-2005; IEEE Standard for Local and Metropolitan Area Networks. Part 16: Air Interface for Fixed Broadband Wireless Access Systems. IEEE: Piscataway, NJ, USA, 2006.
113. Vu, H.L.; Chan, S.; Andrew, L.L. Performance analysis of best-effort service in saturated IEEE 802.16 networks. *IEEE Trans. Veh. Technol.* **2009**, *59*, 460–472. [CrossRef]
114. Pareit, D.; Lannoo, B.; Moerman, I.; Demeester, P. The history of WiMAX: A complete survey of the evolution in certification and standardization for IEEE 802.16 and WiMAX. *IEEE Commun. Surv. Tutor.* **2011**, *14*, 1183–1211. [CrossRef]
115. Pokhrel, S.R.; Williamson, C. Modeling compound TCP over WiFi for IoT. *IEEE/ACM Trans. Netw.* **2018**, *26*, 864–878. [CrossRef]
116. Sheng, Z.; Yang, S.; Yu, Y.; Vasilakos, A.V.; McCann, J.A.; Leung, K.K. A survey on the IETF protocol suite for the internet of things: Standards, challenges, and opportunities. *IEEE Wirel. Commun.* **2013**, *20*, 91–98. [CrossRef]
117. Sharma, V.K.; Shukla, S.S.P.; Singh, V. A tailored Q-Learning for routing in wireless sensor networks. In Proceedings of the 2012 2nd IEEE International Conference on Parallel, Distributed and Grid Computing, Solan, India, 6–8 December 2012; pp. 663–668.
118. Kanellopoulos, D.; Sharma, V.K. Survey on power-aware optimization solutions for MANETs. *Electronics* **2020**, *9*, 1129. [CrossRef]
119. Shang, W.; Yu, Y.; Droms, R.; Zhang, L. Challenges in IoT Networking via TCP/IP Architecture. NDN Technical Report NDN-0038. 2016. Available online: <http://named-data.net/techreports.html> (accessed on 1 February 2023).
120. Iova, O.; Picco, P.; Istomin, T.; Kiraly, C. RPL: The routing standard for the internet of things... or is it? *IEEE Commun. Mag.* **2016**, *54*, 16–22. [CrossRef]
121. Sharma, V.K.; Kumar, M. Adaptive congestion control scheme in mobile ad-hoc networks. *Peer-Peer Netw. Appl.* **2017**, *10*, 633–657. [CrossRef]
122. Sharma, V.K.; Verma, L.P.; Kumar, M. CL-ADSP: Cross-Layer adaptive data scheduling policy in mobile ad-hoc networks. *Future Gener. Comput. Syst.* **2019**, *97*, 530–563. [CrossRef]
123. Verma, L.P.; Sharma, V.K.; Kumar, M.; Kanellopoulos, D.; Mahanti, A. DB-CMT: A new concurrent Multi-path Stream Control Transport Protocol. *J. Netw. Syst. Manag.* **2022**, *30*, 67. [CrossRef]
124. Verma, L.P.; Sharma, V.K.; Kumar, M.; Mahanti, A. An adaptive multi-path data transfer approach for MP-TCP. *Wirel. Netw.* **2022**, *28*, 2185–2212. [CrossRef]
125. ANSI/ASHRAE Standard 135-2004; BACnet: A Data Communication Protocol for Building Automation and Control Networks, Standard 135-2004. American Society of Heating Refrigeration, and Air-Conditioning Engineers Inc.: Atlanta, GA, USA, 2004.
126. Clark, D.D.; Tennenhouse, D.L. Architectural considerations for a new generation of protocols. *ACM SIGCOMM Comput. Commun. Rev.* **1990**, *20*, 200–208. [CrossRef]
127. Tan, K.; Song, J.; Zhang, Q.; Sridharan, M. A compound TCP approach for high-speed and long distance networks. In Proceedings of the IEEE INFOCOM 2006. 25TH IEEE International Conference on Computer Communications, Barcelona, Spain, 23–29 April 2006. [CrossRef]
128. Verma, L.P.; Sharma, V.K.; Kumar, M.; Kanellopoulos, D. A novel delay-based adaptive congestion control TCP variant. *Comput. Electr. Eng.* **2022**, *101*, 108076. [CrossRef]
129. Pokhrel, S.R.; Panda, M.; Vu, H.L.; Mandjes, M. TCP performance over Wi-Fi: Joint impact of buffer and channel losses. *IEEE Trans. Mob. Comput.* **2015**, *15*, 1279–1291. [CrossRef]
130. Pokhrel, S.R.; Vu, H.L.; Criscienti, A.L. Adaptive admission control for IoT applications in home WiFi networks. *IEEE Trans. Mob. Comput.* **2019**, *19*, 2731–2742. [CrossRef]
131. Pokhrel, S.R.; Singh, S. Compound TCP performance for industry 4.0 WiFi: A cognitive federated learning approach. *IEEE Trans. Ind. Inform.* **2020**, *17*, 2143–2151. [CrossRef]
132. Qiu, T.; Chen, N.; Li, K.; Atiquzzaman, M.; Zhao, W. How can heterogeneous internet of things build our future: A survey. *IEEE Commun. Surv. Tutor.* **2018**, *20*, 2011–2027. [CrossRef]
133. Kharrufa, H.; Al-Kashoash, H.A.; Kemp, A.H. RPL-based routing protocols in IoT applications: A review. *IEEE Sens. J.* **2019**, *19*, 5952–5967. [CrossRef]
134. Sharma, V.K.; Verma, L.P.; Kumar, M. A fuzzy-based adaptive energy efficient load distribution scheme in ad-hoc networks. *Int. J. Intell. Syst. Appl.* **2018**, *12*, 72. [CrossRef]
135. Sharma, V.K.; Kumar, M. Adaptive energy efficient load distribution using fuzzy approach. *Adhoc Sens. Wirel. Netw.* **2017**, *39*, 123–166.
136. Reina, D.G.; Toral, S.L.; Barrero, F.; Bessis, N.; Asimakopoulou, E. The role of ad hoc networks in the internet of things: A case scenario for smart environments. In *Internet of Things and Inter-Cooperative Computational Technologies for Collective Intelligence*; Springer: Berlin/Heidelberg, Germany, 2013; pp. 89–113. [CrossRef]
137. Vazifehdan, J.; Prasad, R.V.; Niemegeers, I. Energy-efficient reliable routing considering residual energy in wireless ad hoc networks. *IEEE Trans. Mob. Comput.* **2013**, *13*, 434–447. [CrossRef]
138. Sharma, V.K.; Kumar, M. Adaptive load distribution approach based on congestion control scheme in ad-hoc networks. *Int. J. Electron.* **2019**, *106*, 48–68. [CrossRef]
139. Papandriopoulos, J.; Dey, S.; Evans, J. Optimal and distributed protocols for cross-layer design of physical and transport layers in MANETs. *IEEE/ACM Trans. Netw.* **2008**, *16*, 1392–1405. [CrossRef]
140. Sharma, V.K.; Verma, L.P.; Kumar, M.; Naha, R.K.; Mahanti, A. A-CAFDS: An adaptive-congestion aware Fibonacci sequence based data scheduling policy. *Comput. Commun.* **2020**, *158*, 141–165. [CrossRef]

141. Tian, Y.; Hou, R. An improved AOMDV routing protocol for internet of things. In Proceedings of the 2010 International Conference on Computational Intelligence and Software Engineering, Wuhan, China, 10–12 December 2010; pp. 1–4. [CrossRef]
142. Tseng, C.H. Multipath load balancing routing for Internet of things. *J. Sens.* **2016**, *2016*, 4250746. [CrossRef]
143. Pan, M.S.; Tseng, Y.C. ZigBee and their applications. In *Sensor Networks and Configuration: Fundamentals, Standards, Platforms, and Applications*; Springer: Berlin/Heidelberg, Germany, 2007; pp. 349–368.
144. Sun, J.; Wang, Z.; Wang, H.; Zhang, X. Research on routing protocols based on ZigBee network. In Proceedings of the Third International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP 2007), Kaohsiung, Taiwan, 26–28 November 2007; Volume 1, pp. 639–642. [CrossRef]
145. Fielding, R.; Gettys, J.; Mogul, J.; Frystyk, H.; Masinter, L.; Leach, P.; Lee, B. Hypertext Transfer Protocol—HTTP/1.1. 1999. Available online: <https://www.w3.org/Protocols/rfc2616/rfc2616.html> (accessed on 2 February 2023).
146. Webber, J.; Parastatidis, S.; Robinson, I. *REST in Practice: Hypermedia and Systems Architecture*; O'Reilly Media, Inc.: Sebastopol, CA, USA, 2010.
147. Dizdarevic, J.; Caprio, F.; Jukan, A.; Masip-Bruin, X. A survey of communication protocols for Internet-of-Things and related challenges of fog and cloud computing integration. *ACM Comput. Surv.* **2019**, *51*, 1–29. [CrossRef]
148. Babovic, Z.B.; Protic, J.; Milutinovic, V. Web performance evaluation for Internet of Things applications. *IEEE Access* **2016**, *4*, 6974–6992. [CrossRef]
149. Bormann, C.; Castellani, A.P.; Shelby, Z. CoAP: An application protocol for billions of tiny internet nodes. *IEEE Internet Comput.* **2012**, *16*, 62–67. [CrossRef]
150. OASIS. Message Queuing Telemetry Transport. Available online: <http://mqtt.org> (accessed on 10 February 2023).
151. OPC Foundation. OPC Unified Architecture Specification. 2023. Available online: <https://opcfoundation.org> (accessed on 10 February 2023).
152. XMPP Standards Foundation. Extensible Messaging and Presence Protocol. 2021. Available online: <https://xmpp.org> (accessed on 10 February 2023).
153. OASIS. *OASIS Advanced Message Queuing Protocol (AMQP) Version 1.0—OASIS Standard*; OASIS: Burlington, MA, USA, 2012.
154. Pardo-Castellote, G.; Innovations, R.T.; Chairman, D.D.S. OMG Data Distribution Service: Real-time publish/subscribe becomes a standard. *RTC Mag.* **2005**, *14*, 1–3. Available online: https://www.rti.com/hubfs/docs/reprint_rti.pdf (accessed on 10 February 2023).
155. Glaroudis, D.; Iossifides, A.; Chatzimisios, P. Survey, comparison and research challenges of IoT application protocols for smart farming. *Comput. Netw.* **2020**, *168*, 107037. [CrossRef]
156. Centenaro, M.; Vangelista, L.; Zanella, A.; Zorzi, M. Long-range communications in unlicensed bands: The rising stars in the IoT and smart city scenarios. *IEEE Wirel. Commun.* **2016**, *23*, 60–67. [CrossRef]
157. Leccese, F.; Cagnetti, M.; Trinca, D. A smart city application: A fully controlled street lighting isle based on Raspberry-Pi card, a ZigBee sensor network and WiMAX. *Sensors* **2014**, *14*, 24408–24424. [CrossRef]
158. Sanchez, L.; Muñoz, L.; Galache, J.A.; Sotres, P.; Santana, J.R.; Gutierrez, V.; Ramdhany, R.; Gluhak, A.; Krco, S.; Theodoridis, E.; et al. SmartSantander: IoT experimentation over a smart city testbed. *Comput. Netw.* **2014**, *61*, 217–238. [CrossRef]
159. Vilajosana, I.; Dohler, M. Machine-to-Machine (M2M) communications for smart cities. *Mach.-Mach. (M2M) Commun.* **2015**, *355–373*. [CrossRef]
160. Huang, J.; Xing, C.C.; Shin, S.Y.; Hou, F.; Hsu, C.H. Optimizing M2M communications and quality of services in the IoT for sustainable smart cities. *IEEE Trans. Sustain. Comput.* **2017**, *3*, 4–15. [CrossRef]
161. Silva, B.N.; Khan, M.; Han, K. Towards sustainable smart cities: A review of trends, architectures, components, and open challenges in smart cities. *Sustain. Cities Soc.* **2018**, *38*, 697–713. [CrossRef]
162. Jin, J.; Gubbi, J.; Luo, T.; Palaniswami, M. Network architecture and QoS issues in the internet of things for a smart city. In Proceedings of the 2012 International Symposium on Communications and Information Technologies (ISCIT), Gold Coast, Australia, 2–5 October 2012; pp. 956–961. [CrossRef]
163. Marques, P.; Manfroi, D.; Deitos, E.; Cegoni, J.; Castilhos, R.; Rochol, J.; Pignaton, E.; Kunst, R. An IoT-based smart cities infrastructure architecture applied to a waste management scenario. *Ad Hoc Netw.* **2019**, *87*, 200–208. [CrossRef]
164. Gaur, A.; Scotney, B.; Parr, G.; McClean, S. Smart city architecture and its applications based on IoT. *Procedia Comput. Sci.* **2015**, *52*, 1089–1094. [CrossRef]
165. Gheisari, M.; Pham, Q.V.; Alazab, M.; Zhang, X.; Fernández-Campusano, C.; Srivastava, G. ECA: An edge computing architecture for privacy-preserving in IoT-based smart city. *IEEE Access* **2019**, *7*, 155779–155786. [CrossRef]
166. Saadeh, M.; Sleit, A.; Sabri, K.E.; Almobaideen, W. Hierarchical architecture and protocol for mobile object authentication in the context of IoT smart cities. *J. Netw. Comput. Appl.* **2018**, *121*, 1–19. [CrossRef]
167. Naranjo, P.G.V.; Pooranian, Z.; Shojafar, M.; Conti, M.; Buyya, R. FOCAN: A Fog-supported smart city network architecture for management of applications in the Internet of Everything environments. *J. Parallel Distrib. Comput.* **2019**, *132*, 274–283. [CrossRef]
168. Ortiz, S. Software-Defined Networking: On the verge of a breakthrough? *Computer* **2013**, *46*, 10–12. [CrossRef]
169. AlZoman, R.; Alenazi, M.J. Exploiting SDN to improve QoS of smart city networks against link failures. In Proceedings of the Seventh International Conference on Software Defined Systems (SDS), Paris, France, 20–23 April 2020; pp. 100–106. [CrossRef]

170. Holik, F. Meeting smart city latency demands with SDN. In *Intelligent Information and Database Systems: Recent Developments. ACIIDS 2019. Studies in Computational Intelligence*; Huk, M., Maleszka, M., Szczerbicki, E., Eds.; Springer: Cham, Switzerland, Volume 830. [[CrossRef](#)]
171. Jazaeri, S.S.; Jabbehdari, S.; Asghari, P.; Haj Seyyed Javadi, H. Edge computing in SDN-IoT networks: A systematic review of issues, challenges and solutions. *Clust. Comput.* **2021**, *24*, 3187–3228. [[CrossRef](#)]
172. Liu, J.; Li, Y.; Chen, M.; Dong, W.; Jin, D. Software-defined internet of things for smart urban sensing. *IEEE Commun. Mag.* **2015**, *53*, 55–63. [[CrossRef](#)]
173. Bi, Y.; Lin, C.; Zhou, H.; Yang, P.; Shen, X.; Zhao, H. Time-constrained big data transfer for SDN-enabled smart city. *IEEE Commun. Mag.* **2017**, *55*, 44–50. [[CrossRef](#)]
174. Nguyen, T.G.; Phan, T.V.; Nguyen, B.T.; So-In, C.; Baig, Z.A.; Sanguanpong, S. Search: A collaborative and intelligent NIDs architecture for SDN-based cloud IoT networks. *IEEE Access* **2019**, *7*, 107678–107694. [[CrossRef](#)]
175. Bhushan, B.; Khamparia, A.; Sagayam, K.M.; Sharma, S.K.; Ahad, M.A.; Debnath, N.C. Blockchain for smart cities: A review of architectures, integration trends and future research directions. *Sustain. Cities Soc.* **2020**, *61*, 102360. [[CrossRef](#)]
176. Sharma, P.K.; Park, J.H. Blockchain based hybrid network architecture for the smart city. *Future Gener. Comput. Syst.* **2018**, *86*, 650–655. [[CrossRef](#)]
177. Makhdoom, I.; Zhou, I.; Abolhasan, M.; Lipman, J.; Ni, W. PrivySharing: A blockchain-based framework for privacy-preserving and secure data sharing in smart cities. *Comput. Secur.* **2020**, *88*, 101653. [[CrossRef](#)]
178. Islam, M.J.; Rahman, A.; Kabir, S.; Karim, M.R.; Acharyya, U.K.; Nasir, M.K.; Band, S.S.; Sookhak, M.; Wu, S. Blockchain-SDN-based energy-aware and distributed secure architecture for IoT in smart cities. *IEEE Internet Things J.* **2021**, *9*, 3850–3864. [[CrossRef](#)]
179. Tuballa, M.L.; Abundo, M.L. A review of the development of Smart Grid technologies. *Renew. Sustain. Energy Rev.* **2016**, *59*, 710–725. [[CrossRef](#)]
180. Demertzis, K.; Tsiknas, K.; Taketzis, D.; Skoutas, D.N.; Skianis, C.; Iliadis, L.; Zoiros, K.E. Communication network standards for smart grid infrastructures. *Network* **2021**, *1*, 132–145. [[CrossRef](#)]
181. Bosisio, A.; Berizzi, A.; Morotti, A.; Pegoiani, A.; Greco, B.; Iannarelli, G. IEC 61850-based smart automation system logic to improve reliability indices in distribution networks. In Proceedings of the 2019 IEEE 8th International Conference on Advanced Power System Automation and Protection (APAP), Florence, Italy, 18–20 October 2019; pp. 1219–1222.
182. Girela-López, F.; López-Jiménez, J.; Jiménez-López, M.; Rodríguez, R.; Ros, E.; Díaz, J. IEEE 1588 high accuracy default profile: Applications and challenges. *IEEE Access* **2020**, *8*, 45211–45220. [[CrossRef](#)]
183. Abdrabou, A. A wireless communication architecture for smart grid distribution networks. *IEEE Syst. J.* **2014**, *10*, 251–261. [[CrossRef](#)]
184. Demir, K.; Germanus, D.; Suri, N. Robust QoS-aware communication in the smart distribution grid. *Peer-Peer Netw. Appl.* **2017**, *10*, 193–207. [[CrossRef](#)]
185. Rehmani, M.H.; Davy, A.; Jennings, B.; Assi, C. Software defined networks-based smart grid communication: A comprehensive survey. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 2637–2670. [[CrossRef](#)]
186. Alam, S.; Sohail, M.F.; Ghauri, S.A.; Qureshi, I.M.; Aqdas, N. Cognitive radio based smart grid communication network. *Renew. Sustain. Energy Rev.* **2017**, *72*, 535–548. [[CrossRef](#)]
187. Molokomme, D.N.; Chabalala, C.S.; Bokoro, P.N. A review of cognitive radio smart grid communication infrastructure systems. *Energies* **2020**, *13*, 3245. [[CrossRef](#)]
188. Hu, S.; Chen, X.; Ni, W.; Wang, X.; Hossain, E. Modeling and analysis of energy harvesting and smart grid-powered wireless communication networks: A contemporary survey. *IEEE Trans. Green Commun. Netw.* **2020**, *4*, 461–496. [[CrossRef](#)]
189. Saleem, Y.; Crespi, N.; Rehmani, M.H.; Copeland, R. Internet of things-aided smart grid: Technologies, architectures, applications, prototypes, and future research directions. *IEEE Access* **2019**, *7*, 62962–63003. [[CrossRef](#)]
190. Younus, M.U.; ul Islam, S.; Ali, I.; Khan, S.; Khan, M.K. A survey on software defined networking enabled smart buildings: Architecture, challenges and use cases. *J. Netw. Comput. Appl.* **2019**, *137*, 62–77. [[CrossRef](#)]
191. Minoli, D.; Sohraby, K.; Occhiogrosso, B. IoT considerations, requirements, and architectures for smart buildings—Energy optimization and next-generation building management systems. *IEEE Internet Things J.* **2017**, *4*, 269–283. [[CrossRef](#)]
192. Jia, M.; Komeily, A.; Wang, Y.; Srinivasan, R.S. Adopting Internet of Things for the development of smart buildings: A review of enabling technologies and applications. *Autom. Constr.* **2019**, *101*, 111–126. [[CrossRef](#)]
193. Kumar, A.; Singh, A.; Kumar, A.; Singh, M.K.; Mahanta, P.; Mukhopadhyay, S.C. Sensing technologies for monitoring intelligent buildings: A review. *IEEE Sens. J.* **2018**, *18*, 4847–4860. [[CrossRef](#)]
194. Silva, B.N.; Khan, M.; Han, K. Integration of Big Data analytics embedded smart city architecture with RESTful web of things for efficient service provision and energy management. *Future Gener. Comput. Syst.* **2020**, *107*, 975–987. [[CrossRef](#)]
195. Kumar, A.; Srivastava, V.; Singh, M.K.; Hancke, G.P. Current status of the IEEE 1451 standard-based sensor applications. *IEEE Sens. J.* **2014**, *15*, 2505–2513. [[CrossRef](#)]
196. Kumar, A.; Hancke, G.P. Energy efficient environment monitoring system based on the IEEE 802.15. 4 standard for low cost requirements. *IEEE Sens. J.* **2014**, *14*, 2557–2566. [[CrossRef](#)]
197. du Plessis, R.; Kumar, A.; Hancke, G.P.; Silva, B.J. A wireless system for indoor air quality monitoring. In Proceedings of the IECON 2016—42nd Annual Conference of the IEEE Industrial Electronics Society, Florence, Italy, 23–26 October 2016; pp. 5409–5414.

198. Kularatna, N.; Sudantha, B.H. An environmental air pollution monitoring system based on the IEEE 1451 standard for low cost requirements. *IEEE Sens. J.* **2008**, *8*, 415–422. [CrossRef]
199. Gagliardi, G.; Lupia, M.; Cario, G.; Tedesco, F.; Cicchello Gaccio, F.; Lo Scudo, F.; Casavola, A. Advanced adaptive street lighting systems for smart cities. *Smart Cities* **2020**, *3*, 1495–1512. [CrossRef]
200. Warmerdam, K.; Pandharipande, A. Location data analytics in wireless lighting systems. *IEEE Sens. J.* **2015**, *16*, 2683–2690. [CrossRef]
201. Tiller, D.K.; Guo, X.; Henze, G.P.; Waters, C.E. Validating the application of occupancy sensor networks for lighting control. *Light. Res. Technol.* **2010**, *42*, 399–414. [CrossRef]
202. Byun, J.; Hong, I.; Lee, B.; Park, S. Intelligent household LED lighting system considering energy efficiency and user satisfaction. *IEEE Trans. Consum. Electron.* **2013**, *59*, 70–76. [CrossRef]
203. Higuera, J.; Hertog, W.; Perálvarez, M.; Polo, J.; Carreras, J. Smart lighting system ISO/IEC/IEEE 21451 compatible. *IEEE Sens. J.* **2015**, *15*, 2595–2602. [CrossRef]
204. Tan, Y.K.; Huynh, T.P.; Wang, Z. Smart personal sensor network control for energy saving in DC grid powered LED lighting system. *IEEE Trans. Smart Grid* **2012**, *4*, 669–676. [CrossRef]
205. Chew, I.; Karunatilaka, D.; Tan, C.P.; Kalavally, V. Smart lighting: The way forward? Reviewing the past to shape the future. *Energy Build.* **2017**, *149*, 180–191. [CrossRef]
206. Füchtenhansl, M.; Grosse, E.H.; Glock, C.H. Smart lighting systems: State-of-the-art and potential applications in warehouse order picking. *Int. J. Prod. Res.* **2021**, *59*, 3817–3839. [CrossRef]
207. Kumar, A.; Hancke, G.P. An energy-efficient smart comfort sensing system based on the IEEE 1451 standard for green buildings. *IEEE Sens. J.* **2014**, *14*, 4245–4252. [CrossRef]
208. Kavalionak, H.; Carlini, E. An HVAC regulation architecture for smart building based on weather forecast. In Proceedings of the Economics of Grids, Clouds, Systems, and Services: 15th International Conference, GECON 2018, Pisa, Italy, 18–20 September 2018; Proceedings 15. Springer International Publishing: Berlin/Heidelberg, Germany, 2019; pp. 92–103.
209. Hao, H.; Lin, Y.; Kowli, A.S.; Barooah, P.; Meyn, S. Ancillary service to the grid through control of fans in commercial building HVAC systems. *IEEE Trans. Smart Grid* **2014**, *5*, 2066–2074. [CrossRef]
210. Sun, B.; Luh, P.B.; Jia, Q.S.; Jiang, Z.; Wang, F.; Song, C. Building energy management: Integrated control of active and passive heating, cooling, lighting, shading, and ventilation systems. *IEEE Trans. Autom. Sci. Eng.* **2012**, *10*, 588–602. [CrossRef]
211. Lin, Y.; Barooah, P.; Meyn, S.; Middelkoop, T. Experimental evaluation of frequency regulation from commercial building HVAC systems. *IEEE Trans. Smart Grid* **2015**, *6*, 776–783. [CrossRef]
212. Ma, Y.; Matuško, J.; Borrelli, F. Stochastic model predictive control for building HVAC systems: Complexity and conservatism. *IEEE Trans. Control Syst. Technol.* **2014**, *23*, 101–116. [CrossRef]
213. Javed, A.; Larijani, H.; Ahmadiania, A.; Emmanuel, R.; Mannion, M.; Gibson, D. Design and implementation of a cloud enabled random neural network-based decentralized smart controller with intelligent sensor nodes for HVAC. *IEEE Internet Things J.* **2016**, *4*, 393–403. [CrossRef]
214. Kumar, A.; Kumar, A.; Singh, A. Energy efficient and low cost air quality sensor for smart buildings. In Proceedings of the 2017 3rd International Conference on Computational Intelligence & Communication Technology (CICT), Ghaziabad, India, 9–10 February 2017; pp. 1–4.
215. Kim, J.Y.; Chu, C.H.; Shin, S.M. ISSAQ: An integrated sensing systems for real-time indoor air quality monitoring. *IEEE Sens. J.* **2014**, *14*, 4230–4244. [CrossRef]
216. Lozano, J.; Suárez, J.I.; Arroyo, P.; Ordiales, J.M.; Alvarez, F. Wireless sensor network for indoor air quality monitoring. *Chem. Eng. Trans.* **2012**, *30*, 231–235.
217. Bhattacharya, S.; Sridevi, S.; Pitchiah, R. Indoor air quality monitoring using wireless sensor network. In Proceedings of the 2012 Sixth International Conference on Sensing Technology (ICST), Kolkata, India, 18–21 December 2012; pp. 422–427.
218. Kim, D.; Yoon, Y.; Lee, J.; Mago, P.J.; Lee, K.; Cho, H. Design and implementation of smart buildings: A review of current research trend. *Energies* **2022**, *15*, 4278. [CrossRef]
219. Metallidou, C.K.; Psannis, K.E.; Egyptiadou, E.A. Energy efficiency in smart buildings: IoT approaches. *IEEE Access* **2020**, *8*, 63679–63699. [CrossRef]
220. Mariano-Hernández, D.; Hernández-Callejo, L.; Zorita-Lamadrid, A.; Duque-Pérez, O.; García, F.S. A review of strategies for building energy management system: Model predictive control, demand side management, optimization, and fault detect & diagnosis. *J. Build. Eng.* **2021**, *33*, 101692. [CrossRef]
221. Moudgil, V.; Hewage, K.; Hussain, S.A.; Sadiq, R. Integration of IoT in building energy infrastructure: A critical review on challenges and solutions. *Renew. Sustain. Energy Rev.* **2023**, *174*, 113121. [CrossRef]
222. The Smart Water Networks Forum What Is a Smart Water Network? Available online: <https://swan-forum.com/smart-water-network/> (accessed on 1 October 2022).
223. Nguyen, K.A.; Stewart, R.A.; Zhang, H.; Sahin, O.; Siriwardene, N. Re-engineering traditional urban water management practices with smart metering and informatics. *Environ. Model. Softw.* **2018**, *101*, 256–267. [CrossRef]
224. Chen, Y.; Han, D. Water quality monitoring in smart city: A pilot project. *Autom. Constr.* **2018**, *89*, 307–316. [CrossRef]
225. Kamienski, C.; Soirinen, J.P.; Taumberger, M.; Dantas, R.; Toscano, A.; Cinotti, T.S.; Maia, R.F.; Neto, A.T. Smart water management platform: IoT-based precision irrigation for agriculture. *Sensors* **2019**, *19*, 276. [CrossRef]

226. Ye, Y.; Liang, L.; Zhao, H.; Jiang, Y. The System Architecture of Smart Water Grid for Water Security. *Procedia Eng.* **2016**, *154*, 361–368. [[CrossRef](#)]
227. Alvisi, S.; Casellato, F.; Franchini, M.; Govoni, M.; Luciani, C.; Poltronieri, F.; Riberto, G.; Stefanelli, C.; Tortonesi, M. Wireless middleware solutions for smart water metering. *Sensors* **2019**, *19*, 1853. [[CrossRef](#)] [[PubMed](#)]
228. Li, J.; Yang, X.; Sitzenfrei, R. Rethinking the framework of smart water system: A review. *Water* **2020**, *12*, 412. [[CrossRef](#)]
229. Dong, X.; Lin, H.; Tan, R.; Iyer, R.K.; Kalbarczyk, Z. Software-Defined Networking for Smart Grid Resilience: Opportunities and Challenges. In Proceedings of the CPSS 2015—1st ACM Workshop on Cyber-Physical System Security, Part of ASIACCS 2015, Denver, CO, USA, 16 October 2015; pp. 61–68. [[CrossRef](#)]
230. Luciani, C.; Casellato, F.; Alvisi, S.; Franchini, M. From Water Consumption Smart Metering to Leakage Characterization at District and User Level: The GST4Water Project. *Proceedings* **2018**, *2*, 675. [[CrossRef](#)]
231. Panagiotakopoulos, T.; Vlachos, D.P.; Bakalakos, T.V.; Kanavos, A.; Kameas, A. A FIWARE-based IoT framework for smart water distribution management. In Proceedings of the 12th International Conference on Information, Intelligence, Systems & Applications (IISA), Chania Crete, Greece, 12–14 July 2021; pp. 1–6. [[CrossRef](#)]
232. Amaxilatis, D.; Chatzigiannakis, I.; Tselios, C.; Tsironis, N.; Niakas, N.; Papadogeorgos, S. A smart water metering deployment based on the fog computing paradigm. *Appl. Sci.* **2020**, *10*, 1965. [[CrossRef](#)]
233. Kulkarni, P.; Farnham, T. Smart city wireless connectivity considerations and cost analysis: Lessons learnt from smart water case studies. *IEEE Access* **2016**, *4*, 660–672. [[CrossRef](#)]
234. Watson, J.P.; Greenberg, H.J.; Hart, W.E. A multiple-objective analysis of sensor placement optimization in water networks. In *Critical Transitions in Water and Environmental Resources Management*; American Society of Civil Engineers: Reston, VA, USA, 2004; pp. 1–10.
235. Berry, J.W.; Fleischer, L.; Hart, W.E.; Phillips, C.A.; Watson, J.P. Sensor placement in municipal water networks. *J. Water Resour. Plan. Manag.* **2005**, *131*, 237–243. [[CrossRef](#)]
236. Liu, S.; Liu, W.; Chen, J.; Wang, Q. Optimal locations of monitoring stations in water distribution systems under multiple demand patterns: A flaw of demand coverage method and modification. *Front. Environ. Sci. Eng.* **2012**, *6*, 204–212. [[CrossRef](#)]
237. Whittle, A.J.; Girod, L.; Preis, A.; Allen, M.; Lim, H.B.; Iqbal, M.; Srirangarajan, S.; Fu, C.; Wong, K.J.; Goldsmith, D. WATER-WISE@SG: A testbed for continuous monitoring of the water distribution system in Singapore. In *Water Distribution Systems Analysis*; American Society of Civil Engineers: Reston, VA, USA, 2010; pp. 1362–1378.
238. Whittle, A.; Allen, M.; Preis, A.; Iqbal, M. Sensor networks for monitoring and control of water distribution systems. In Proceedings of the 6th International Conference on Structural Health Monitoring of Intelligent Infrastructure, Hong Kong, China, 9–11 December 2013; pp. 9–11.
239. Patil, K.; Ghosh, A.; Das, D.; Vuppala, S.K. IWCMSE: Integrated water consumption monitoring solution for enterprises. In Proceedings of the ACM International Conference on Interdisciplinary Advances in Applied Computing, Amritapuri, India, 10–14 October 2014; pp. 1–8. [[CrossRef](#)]
240. Yoon, S.; Ye, W.; Heidemann, J.; Littlefield, B.; Shahabi, C. SWATS: Wireless sensor networks for steamflood and waterflood pipeline monitoring. *IEEE Netw.* **2011**, *25*, 50–56. [[CrossRef](#)]
241. Ang, L.M.; Seng, K.P.; Ijemaru, G.K.; Zungeru, A.M. Deployment of IoV for smart cities: Applications, architecture, and challenges. *IEEE Access* **2018**, *7*, 6473–6492. [[CrossRef](#)]
242. Liu, K.; Xu, X.; Chen, M.; Liu, B.; Wu, L.; Lee, V.C. A hierarchical architecture for the future internet of vehicles. *IEEE Commun. Mag.* **2019**, *57*, 41–47. [[CrossRef](#)]
243. Chen, M.; Tian, Y.; Fortino, G.; Zhang, J.; Humar, I. Cognitive internet of vehicles. *Comput. Commun.* **2018**, *120*, 58–70. [[CrossRef](#)]
244. Karim, A. Development of secure Internet of Vehicle Things (IoVT) for smart transportation system. *Comput. Electr. Eng.* **2022**, *102*, 108101. [[CrossRef](#)]
245. Contreras-Castillo, J.; Zeadally, S.; Guerrero-Ibañez, J.A. Internet of vehicles: Architecture, protocols, and security. *IEEE Internet Things J.* **2017**, *5*, 3701–3709. [[CrossRef](#)]
246. Ji, B.; Zhang, X.; Mumtaz, S.; Han, C.; Li, C.; Wen, H.; Wang, D. Survey on the internet of vehicles: Network architectures and applications. *IEEE Commun. Stand. Mag.* **2020**, *4*, 34–41. [[CrossRef](#)]
247. Sharma, P.K.; Moon, S.Y.; Park, J.H. Block-VN: A distributed blockchain based vehicular network architecture in smart city. *J. Inf. Process. Syst.* **2017**, *13*, 184–195. [[CrossRef](#)]
248. Jan, B.; Farman, H.; Khan, M.; Talha, M.; Din, I.U. Designing a smart transportation system: An internet of things and big data approach. *IEEE Wirel. Commun.* **2019**, *26*, 73–79. [[CrossRef](#)]
249. Saxena, D.; Raychoudhury, V.; Suri, N.; Becker, C.; Cao, J. Named Data Networking: A survey. *Comput. Sci. Rev.* **2016**, *19*, 15–55. [[CrossRef](#)]
250. Kaiwartya, O.; Abdullah, A.H.; Cao, Y.; Altameem, A.; Prasad, M.; Lin, C.T.; Liu, X. Internet of vehicles: Motivation, layered architecture, network model, challenges, and future aspects. *IEEE Access* **2016**, *4*, 5356–5373. [[CrossRef](#)]
251. Kerrache, C.A.; Lagraa, N.; Hussain, R.; Ahmed, S.H.; Benslimane, A.; Calafate, C.T.; Cano, J.-C.; Vegni, A.M. TACASHI: Trust-aware communication architecture for social internet of vehicles. *IEEE Internet Things J.* **2019**, *6*, 5870–5877. [[CrossRef](#)]
252. Anastasiou, E.; Manika, S.; Ragazou, K.; Katsios, I. Territorial and human geography challenges: How can Smart villages support rural development and population inclusion? *Soc. Sci.* **2021**, *10*, 193. [[CrossRef](#)]
253. Komorowski, Ł.; Stanny, M. Smart villages: Where can they happen? *Land* **2020**, *9*, 151.

254. Cambra-Fierro, J.J.; Pérez, L. (Re) thinking smart in rural contexts: A multi-country study. *Growth Chang.* **2022**, *53*, 868–889. [[CrossRef](#)]
255. European Network for Rural Development, Smart Villages. Available online: https://enrd.ec.europa.eu/smart-and-competitive-rural-areas/smart-villages_en (accessed on 10 June 2022).
256. IEEE Smart Village. Available online: <http://ieee-smart-village.org/> (accessed on 10 June 2022).
257. Malik, P.K.; Singh, R.; Gehlot, A.; Akram, S.V.; Das, P.K. Village 4.0: Digitalization of village with smart internet of things technologies. *Comput. Ind. Eng.* **2022**, *165*, 107938. [[CrossRef](#)]
258. Shrestha, S.; Drozdenko, B. Smart Rural Framework using IoT devices and Cloud computing. In Proceedings of the 2019 IEEE Green Technologies Conference (GreenTech), Lafayette, LA, USA, 3–6 April 2019. [[CrossRef](#)]
259. Monzon Baeza, V.; Alvarez Marban, M. High Altitude Platform Stations Aided Cloud-Computing Solution for Rural-Environment IoT Applications. *Comput. Netw. Commun.* **2022**, *1*, 85–98.
260. Aljuhani, A.; Kumar, P.; Kumar, R.; Jolfaei, A.; Islam, A.N. Fog intelligence for secure smart villages: Architecture, and future challenges. *IEEE Consum. Electron. Mag.* **2022**, *8*, 1–9. [[CrossRef](#)]
261. Rohan, R.; Pal, D.; Watanapa, B.; Funikul, S. Emerging Paradigm of IoT Enabled Smart Villages. In Proceedings of the 2022 IEEE International Conference on Consumer Electronics (ICCE), Las Vegas, NV, USA, 7–9 January 2022.
262. Han, B.; Gopalakrishnan, V.; Ji, L.; Lee, S. Network function virtualization: Challenges and opportunities for innovations. *IEEE Commun. Mag.* **2015**, *53*, 90–97. [[CrossRef](#)]
263. Li, Y.; Chen, M. Software-defined network function virtualization: A survey. *IEEE Access* **2015**, *3*, 2542–2553. [[CrossRef](#)]
264. Sinh, D.; Le, L.V.; Lin, B.S.P.; Tung, L.P. SDN/NFV—A new approach of deploying network infrastructure for IoT. In Proceedings of the 2018 27th Wireless and Optical Communication Conference (WOCC), Hualien, Taiwan, 30 April–1 May 2018; pp. 1–5.
265. Mukherjee, B.K.; Pappu, S.I.; Islam, M.; Acharyya, U.K. An SDN based distributed IoT network with NFV implementation for smart cities. In Proceedings of the International Conference on Cyber Security and Computer Science, Dhaka, Bangladesh, 15–16 February 2020; Springer: Cham, Switzerland; pp. 539–552. [[CrossRef](#)]
266. Khan, A.A.; Rehmani, M.H.; Rachedi, A. Cognitive-radio-based Internet of Things: Applications, architectures, spectrum related functionalities, and future research directions. *IEEE Wirel. Commun.* **2017**, *24*, 17–25. [[CrossRef](#)]
267. Pranaya, Y.C.; Himarish, M.N.; Baig, M.N.; Ahmed, M.R. Cognitive architecture based smart grids for smart cities. In Proceedings of the 3rd International Conference on Power Generation Systems and Renewable Energy Technologies (PGSRET 2017), Johor Bahru, Malaysia, 4–6 April 2017; pp. 44–49. [[CrossRef](#)]
268. Gai, K.; Xu, K.; Lu, Z.; Qiu, M.; Zhu, L. Fusion of cognitive wireless networks and edge computing. *IEEE Wirel. Commun.* **2019**, *26*, 69–75. [[CrossRef](#)]
269. Scrugli, M.A.; Loi, D.; Raffo, L.; Meloni, P. A runtime-adaptive cognitive IoT node for healthcare monitoring. In Proceedings of the 16th ACM International Conference on Computing Frontiers 2019, Alghero, Italy, 30 April–2 May 2019; pp. 350–357. [[CrossRef](#)]
270. Li, F.; Lam, K.Y.; Li, X.; Sheng, Z.; Hua, J.; Wang, L. Advances and emerging challenges in cognitive internet-of-things. *IEEE Trans. Ind. Inform.* **2019**, *16*, 5489–5496. [[CrossRef](#)]
271. Park, J.H.; Salim, M.M.; Jo, J.H.; Sicato, J.C.S.; Rathore, S.; Park, J.H. CIoT-Net: A scalable cognitive IoT based smart city network architecture. *Hum.-Cent. Comput. Inf. Sci.* **2019**, *9*, 29. [[CrossRef](#)]
272. Nayak, P.; Garetto, M.; Knightly, E.W. Multi-user downlink with single-user uplink can starve TCP. In Proceedings of the IEEE INFOCOM 2017, Atlanta, GA, USA, 1–4 May 2017; pp. 1–9. [[CrossRef](#)]
273. Bejarano, O.; Knightly, E.W.; Park, M. IEEE 802.11 ac: From channelization to multi-user MIMO. *IEEE Commun. Mag.* **2013**, *51*, 84–90. [[CrossRef](#)]
274. Pokhrel, S.R.; Choi, J. Improving TCP performance over WiFi for internet of vehicles: A federated learning approach. *IEEE Trans. Veh. Technol.* **2020**, *69*, 6798–6802. [[CrossRef](#)]
275. Rhee, I.; Xu, L.; Ha, S.; Zimmermann, A.; Eggert, L.; Scheffenegger, R. CUBIC for Fast Long-Distance Networks (No. Rfc8312). 2018. Available online: <https://www.rfc-editor.org/rfc/rfc8312> (accessed on 1 February 2023).
276. Shahraki, A.; Taherkordi, A.; Haugen, Ø.; Eliassen, F. A survey and future directions on clustering: From WSNs to IoT and modern networking paradigms. *IEEE Trans. Netw. Serv. Manag.* **2020**, *18*, 2242–2274. [[CrossRef](#)]
277. Mylonas, G.; Kalogerias, A.; Kalogerias, G.; Anagnostopoulos, C.; Alexakos, C.; Munoz, L. Digital twins from smart manufacturing to smart cities: A survey. *IEEE Access* **2021**, *9*, 143222–143249. [[CrossRef](#)]
278. Akhtar, M.W.; Hassan, S.A.; Ghaffar, R.; Jung, H.; Garg, S.; Hossain, M.S. The shift to 6G communications: Vision and requirements. *Hum. Cent. Comput. Inf. Sci.* **2020**, *10*, 53. [[CrossRef](#)]
279. Nguyen, V.L.; Lin, P.C.; Cheng, B.C.; Hwang, R.H.; Lin, Y.D. Security and privacy for 6G: A survey on prospective technologies and challenges. *IEEE Commun. Surv. Tutor.* **2021**, *23*, 2384–2428. [[CrossRef](#)]
280. Farooq, M.S.; Nadir, R.M.; Rustam, F.; Hur, S.; Park, Y.; Ashraf, I. Nested Bee Hive: A conceptual multilayer architecture for 6G in futuristic sustainable smart cities. *Sensors* **2022**, *22*, 5950. [[CrossRef](#)] [[PubMed](#)]
281. Huang, H.; Guo, S.; Gui, G.; Yang, Z.; Zhang, J.; Sari, H.; Adachi, F. Deep learning for physical-layer 5G wireless techniques: Opportunities, challenges and solutions. *IEEE Wirel. Commun.* **2020**, *27*, 214–222. [[CrossRef](#)]
282. Chen, M.; Challita, U.; Saad, W.; Yin, C.; Debbah, M. Artificial Neural Networks-Based Machine Learning for Wireless Networks: A Tutorial. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 3039–3071. [[CrossRef](#)]
283. Manzalini, A. Quantum Communications in Future Networks and Services. *Quantum Rep.* **2020**, *2*, 221–232. [[CrossRef](#)]

284. Tariq, F.; Khandaker, M.R.A.; Wong, K.K.; Imran, M.A.; Bennis, M.; Debbah, M. A speculative study on 6G. *IEEE Wirel. Commun.* **2020**, *27*, 118–125. [[CrossRef](#)]
285. Imoize, A.L.; Adedeji, O.; Tandiya, N.; Shetty, S. 6G enabled smart infrastructure for sustainable society: Opportunities, challenges, and research roadmap. *Sensors* **2021**, *21*, 1709. [[CrossRef](#)] [[PubMed](#)]
286. Basar, E.; Di Renzo, M.; De Rosny, J.; Debbah, M.; Alouini, M.-S.; Zhang, R. Wireless communications through Reconfigurable Intelligent Surfaces. *IEEE Access* **2019**, *7*, 116753–116773. [[CrossRef](#)]
287. Hu, S.; Rusek, F.; Edfors, O. Beyond Massive MIMO: The potential of data transmission with large intelligent surfaces. *IEEE Trans. Signal Process.* **2018**, *66*, 2746–2758. [[CrossRef](#)]
288. Akyildiz, I.F.; Kak, I.A. The Internet of Space Things/Cubesats. *IEEE Netw.* **2019**, *33*, 212–218. [[CrossRef](#)]
289. Akyildiz, I.F.; Jornet, J.M.; Han, C. Terahertz band: Next frontier for wireless communications. *Phys. Commun.* **2014**, *12*, 16–32. [[CrossRef](#)]
290. Kumari, A.; Gupta, R.; Tanwar, S. Amalgamation of blockchain and IoT for smart cities underlying 6G communication: A comprehensive review. *Comput. Commun.* **2021**, *172*, 102–118. [[CrossRef](#)]
291. Kamruzzaman, M.M. Key technologies, applications and trends of internet of things for energy-efficient 6G wireless communication in smart cities. *Energies* **2022**, *15*, 5608. [[CrossRef](#)]
292. Kohli, V.; Tripathi, U.; Chamola, V.; Rout, B.K.; Kanhere, S.S. A review on Virtual Reality and Augmented Reality use-cases of Brain Computer Interface based applications for smart cities. *Microprocess. Microsyst.* **2022**, *88*, 104392. [[CrossRef](#)]

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