Wireless Technology for Smart Cities and Urban Planning

Abstract

This chapter provides a comprehensive overview of wireless communication technologies related to IoT applications in smart cities and urban planning. In this context, it explains various wireless technologies used in IoT for smart cities and urban planning including Wi-Fi, Zigbee, LoRa, cellular networks (4G/5G), Bluetooth and other emerging standards, including the strengths and weaknesses of each protocol. It covers the fundamental theory of IoT and its architecture. The scope of the chapter covers various IoT applications in urban planning. This work emphasizes on the role of IoT in various aspects of urban planning, including transportation, energy management, environmental monitoring, public safety and infrastructure optimization. It highlights the transformative impact of wireless IoT technologies on urban development. The chapter also discusses various challenges with their advanced solutions in implementing IoT in smart cities.

Keywords: Wireless technologies; IoT; Smart Cities; Urban Planning

Authors

Dr. Gunjan Mittal Roy
IILM University, Greater Noida campus
Greater Noida, India
gunjan.mittal@iilm.edu

Dr. Sambhavi Shukla
IILM University, Greater Noida campus
Greater Noida, India
sambhavi.shukla@iilm.edu

Corresponding Author

Dr. Damyanti Singh
IILM University
Greater Noida campus
Greater Noida, India
damyanti.singh@iilm.edu

I. INTRODUCTION

The growth of wireless technologies integrated with the Internet of Things (IoT) and Cloud computing has stimulated the development of smart cities and refurbished urban planning. This is because of faster communication and greater connectivity among the citizens in public spaces. The socio-economic definition of a smart city largely spans across building secure and adequate infrastructure. Efficient health sector and smart education are also some of the important indicators that need constant upgradation. It is these sensitive domains that call for immediate action on wireless sensor networks. The purpose of this study is to educate readers about wireless IoT technologies to provide a clear and accessible explanation of the various wireless technologies involved in IoT applications. The motivation for writing this chapter is to ensure that readers gain a solid understanding of the capabilities and limitations of each technique. In addition, it also shows the role of IoT in urban planning, showing the ways in which IoT promotes urban planning goals such as sustainability, efficiency and quality of life. The purpose of this chapter is to cover the challenges and solutions in this area. Raise awareness of the challenges of implementing wireless IoT in urban environments, offering practical solutions and strategies to address these challenges, encouraging problem solving. It also focuses on an overview of future trends. Section II of the chapter consists of the Wireless technologies in IoT and urban planning, section III covers the IoT Fundamentals and Architecture in Smart Cities, section IV focuses on the IoT Applications in Urban Planning, section V deals with the Challenges in Implementation of IoT (Internet of Things) in smart cities and urban planning with the respective solutions, section VI discusses about advanced solutions and innovations, section VII focuses on future trends and development of wireless technology and finally section VIII brings out the conclusion of the work.

Wireless technologies are the backbone of smart cities. Building a robust and high-speed wireless network is a quintessential step towards modern urban planning. A smart city is defined as the convergence of IOT and AI techniques built over wireless technologies. Wireless technologies have presented themselves as a solution to the rapid growth of devices that are connected to the network as well as the increasing demand of services that allow monitoring cities. IoT is gaining rapid popularity and it is being utilized for transport, health, environment, animal monitoring and smart metering applications [4,5]. Wireless technologies are varied and their utilization should be considered depending on the application. Some applications of wireless technology in smart cities are shown in Fig.1. Traffic type, distance, energy consumption or number of nodes are some of the factors that should be considered when deciding how to transmit the gathered data. Wireless Sensor Networks (WSNs) are discussed in the reported works with the approach being dependent on transmission, processing or the network itself which is shown in Fig.2. These networks are being employed all over the world as a low-cost and low-energy consuming method to provide a communication mechanism [6]. Wireless networks play a significant role at the time of first responders in the field operations. For emergency medical service, broadband data rate is required. This application highlights the sensitivity of an efficient wireless network [1]. Various algorithms are also reported in the past that act as a pre-encoder in the wireless surveillance systems. These applications require a trade-off between complexity of the coding modules and accurate object detection [2]. At the same time, the wireless video surveillance systems (WVSS) are highly susceptible to cyber- attacks. IoT-fuzzy inference system-based jamming detection system for detecting the presence of jamming [cited]. The efficiency of

these proposed models is compared in detecting jamming signals. For example, for efficient transmission of power in a typical smart city, smart grids are utilized that are tapping the potential of IoT [3]. Utilizing the GPRS (General Packet radio Services) technology, one is able to identify the motion detection and accordingly send the snapshots to the server [4]. Défense artillery like drones and automatic missiles will eventually make IoT the heart of autonomy, which in turn will require ultra-reliable wireless networks.

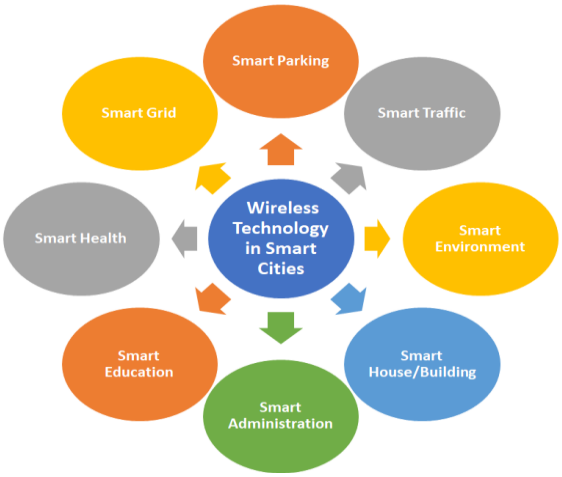

Figure 1: Applications of Wireless Technology in Smart Cities

Wireless technologies also depend on the environmental conditions and the parameters that are subject to change. For example, the education sector requires shorter ranges and higher bandwidth, while the agriculture domain needs long-distance communication [5]. The recent standards use IEEE 802.15.1 for the short-range wireless communication and low cost, but, at the cost of lower reliability and lower data rates [6]. Whereas, WiMax is employed for long distance communication. The sensors used in the smart cities store and process the acquired data to the cloud platforms. Even they require efficient and intelligent wireless services for the smooth flow of sensitive information [7]. Various IoT protocols use different wireless technologies depending on the usage in the real-world. Be it home automation, industrial automation or health care services. IoT networking technologies are also employed depending on the IoT architecture. For example, network layer encapsulation protocol uses Zigbee IP, while the data link layer protocol uses IEEE 802.15.4e [8].

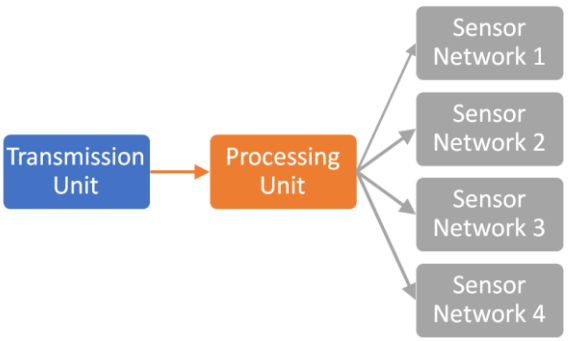

Figure 2: General Diagram of Wireless Sensor Networks

To build intelligent, adaptable and secure workplaces, wireless technologies, however efficient, are still in dire need of technological advancements like ICT and Artificial Intelligence and Machine Learning and Big Data Analytics, shown in Fig.3. The ML algorithms for communications should dynamically adapt to learn complex models that underlie wireless networks and devices. Rigorous research is underway for developing light-weight ML algorithms, especially deep learning models, for embedded systems [9]. An important application of AI and ML is to exploit big data analytics to enhance situational awareness and overall network operation. Herein, AI will provide the wireless network with the ability to parse through massive amounts of data, generated from multiple sources that range from wireless channel measurements and sensor readings to drones and surveillance images, in order to create a comprehensive map of a large number of devices within the network [10]. Data aggregation algorithm based on the Markov chain is used to resend the data after it fails to transmit the first time. This rectifies the issues that the sensor faces in an unreliable communication environment due to information transmission failure. The experimental results show that the system can realize information sharing, exchange and fusion between various sensing subsystems, solve the previous information island phenomenon and meet the actual needs of smart cities [11]. Moreover, the abuse of wireless technologies may derive in some domains. In the context of AI for IoT security, there will always be a challenge to generate high quality training data sets, keeping in account the large number of devices that are continuously generating large volumes of data. For the many challenges seen in the globally optimized network, there are reported works that account for localized IOT based AI yielding benefits such as low bandwidth and latency issues [12]. Apple's Bluetooth feature of Live in, although comes with many unique advantages. However, it has the ability to listen to the sounds picked up by the phone. There are ample reports regarding hidden wireless cameras whose data can be recorded and directly accessed via smartphones. There is still limited research discussing the efficacy of detection tools to find the hidden wireless devices [13]. Rapid advancements in the field of emerging IoT techniques equally require attention towards IoT security parameters such as data authentication, protection and scalability. Hacking techniques such as Man in the middle attack, placing the attacker's device between the target IoT device and the intended receiver, this attack can be carried out in an IoT system, giving the attacker access to the communication between these two devices. Apart from this, Malware and Distributed Denial of Services are also some of the challenges faced by IoT security [14].

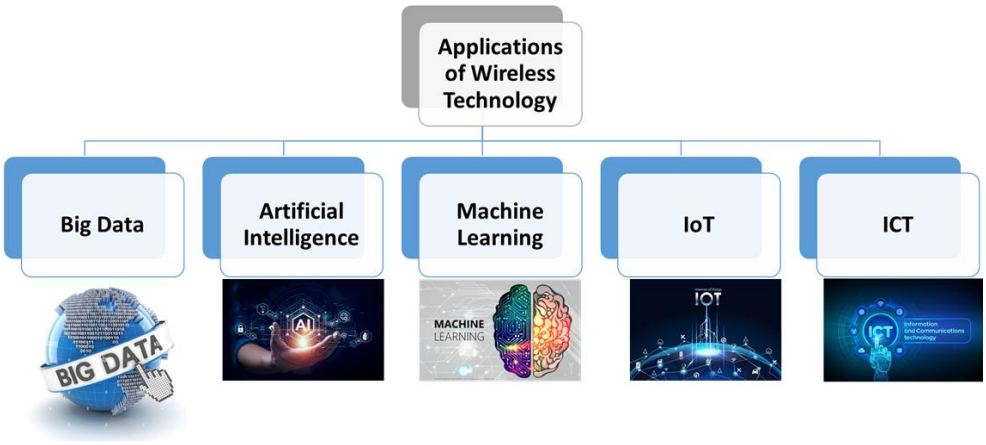

Figure 3: Applications of Wireless Technology

Since wireless transmissions are broadcast, the data being transferred is vulnerable to eavesdropping. For the secure data transition, new threats are motivating the organizations to secure not only their office environments but also individual employees working from home during the pandemic. This has caused maintaining cyber security costly and challenging, especially for smaller firms. A review paper recently listed the major security and privacy challenges incurred by the existing wireless networks [15]. Efficient routing protocols have been designed in order to enhance the efficiency with which the packets are being transmitted. Shanthi et al., have proposed a multi-link routing protocol combined with blowfish mode, so as to create a safe transmission of private data to travel among different sensor nodes. The proposed protocol designs are shown to have achieved better performance metrics in terms of data transfer rate, power consumption and latency [16]. Among the authentication protocols, lightweight authentication protocols, key management protocols as well as broadcast authentication protocols have the advantage of reduced computation overhead and minimum memory utilization, when applied to various applications, as listed by S. Raja Rajeswari and V. Seenivasagam [17].

The following technical research has to be enhanced in order to further advance the field of intelligent city information systems study: (1) System for the Internet of Things; (2) Information fusion from several sensors; (3) Sensing technology with intelligence; (4) Industry 4.05 Internet +. We think that in the future, smart cities will be much smarter and more efficient, as they are already steadily improving our lives [11]. Laser Power Transmission (LPT) provides increased safety, high efficiency, and contactless transmission. With the use of this technology, energy transmission efficiency could be greatly increased, energy loss could be decreased, and pollution to the environment could be reduced. Furthermore, LPT can give wireless power to robots, aerospace vehicles, and mobile devices, improving the lifespan and dependability of these systems. Here, this cutting-edge technology has the potential to completely transform the transmission and use of power, leading to significant advancements for the energy industry in the future [18]. Additionally, there is an equal need to develop eco-friendly and sustainable IoT. Various potential solutions towards building a “green IoT” have been listed by Alsharif et al. The energy-aware routing protocol, or EARP, is a "smart" routing technique intended for Internet of Things networks that possess the ability to harvest energy. Based on the energy availability and network characteristics of individual nodes, EARP uses a decentralized technique to dynamically modify network paths. Another illustration is the e-traffic-aware energy-efficient routing (TEER) protocol, which is intended for Internet of Things networks with constrained energy supplies. In order to dynamically modify network paths in response to traffic patterns and energy availability, TEER employs a centralized methodology [19].

II. WIRELESS TECHNOLOGIES IN IOT AND URBAN PLANNING

Wireless technologies play a crucial role in facilitating Internet of Things (IoT) applications in smart cities and urban planning. These technologies provide the connectivity infrastructure necessary for IoT devices and sensors to communicate, share data, and contribute to the development of intelligent urban environments. The most popularly used wireless technologies in the domain of IoT and urban planning are shown in Fig.4.

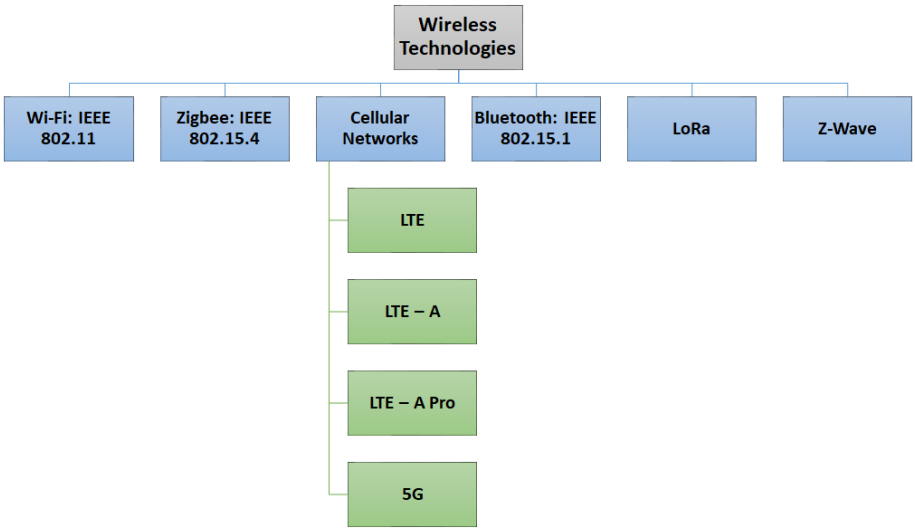

Figure 4: Types of Wireless Technologies used in IoT and Urban Planning

1. **Wi-Fi: IEEE 802.11:** The most popular standards for home and business settings to enable internet connectivity for a multitude of devices are Wi Fi. It is also being used to deploy access points throughout the city to give residents free internet access. Wi Fi allows the transmission of all kinds of data, albeit high-quality multimedia traffic may prove to be problematic for older iterations of the standard. The bit rates for IEEE 802.11 have been rising since the introduction of wireless technologies and their new standards. For example, the speed of the wireless standard 802.15.4 is just 250 kbps, whereas the speed of 802.11AD is 7 Mbps. As a result, users can move about easily and seamlessly when connecting to different network access points. The drawbacks of this technology are its restricted service radius, considerable signal attenuation, and less reliable Wi Fi connections than cable ones [20]. The inside coverage area of the Wi Fi radius is 20–70 meters, while the outside radius is between 100 and 250 meters. This indicates that the Wi Fi radius has a medium range. So, only the devices themselves can move away inside specified ranges. Every Wi Fi standard uses a different frequency range, ranging from 2.4 GHz to 5 GHz. The IEEE 802.11b standard has a better signal over extended distances than the IEEE 802.11a/b/n/g standards. The better ones at close ranges are IEEE 802.11b and IEEE 802.11n [21, 22]. It may be particularly relevant to a smart city's infrastructure, population, governance, and economics.

    - **Zigbee: IEEE 802.15.4/ ZigBee:** This working group was established in 2003 with the goal of standardizing WPAN[23]. This wireless technology's goal is to enable communication between several devices within a 10-meter operational range while consuming the least amount of power possible while being tiny in size and inexpensive. The main benefit is that it may be used with devices that don't require fast data transfer speeds and have a battery life of several months or years. The IEEE 802.15.4-2006 and IEEE 802.15.4-2011 modifications were introduced in 2006 and 2011, respectively [24]. The most recent one defines 12 PHY alternatives, the most commonly used of which is the 2450 direct-sequence spread spectrum (DSSS). IEEE 802.15.4 supports a variety of personal area networks (PANs), including beacon-enabled PANs and PAN without beacon capability.

Carrier Sense Multiple Access with Collision Avoidance (CSMA-CA) is the channel access technique used by non-beacon-enabled PANs, whereas slotted CSMA-CA is used by beacon-enabled PANs. The IEEE 802.15.4 standard and the ZigBee technology are quite similar. Unlike IEEE 802.15.4, which describes the communication of the second level, it explains the communication in the third level of the OSI (Open System Interconnection) architecture. ZigBee can be used to operate two different kinds of devices: full-function devices (FFD) and reduced-function devices (RFD). The RFD is mainly meant for basic tasks like light switches or passive sensors; on the other hand, the FFD can function as a PAN coordinator and connect with both FFD and RFD. In order to prevent conflicts with other PANs in the same area, an FFD can establish its own network, take on the role of PAN coordinator, and choose a PAN ID in order to avoid conflicts with other PANs in the same area. The three topologies that can be used with ZigBee are cluster topology, peer-to-peer topology, and both.

2. **Cellular Networks (4G/5G):** The term "4G" refers to the fourth generation of cellular communication protocols. The 2G and 3G mobile standard families have replaced it. By providing a comprehensive and dependable IP-based solution for voice, data, and multimedia, 4G technology enhances current communication networks. In comparison to earlier generations, subscribers can access this system at any time, from any location, and at far higher data speeds. Digital Video Broadcasting (DVB), Multimedia Messaging Service (MMS), High-Definition TV, and mobile TV are some of the applications that are being developed to utilize a 4G network. For extremely mobile scenarios, such as receiving service from a moving vehicle or train, 4G may deliver 100 Mb per second.1 Gb per seconds for low mobility like when walking (pedestrian) [25].

    - **LTE:** 3GPP radio interface makes up LTE. It uses novel modulation techniques to boost data speed and capacity. It is based on GSM/EDGE and UMTS/HSPA mobile network technology. The frequency division and time division duplexing are supported, and the carrier bandwidths range from 1.4 MHz to 20 MHz. As a result, it offers peak download rates of 300 megabits per second and upload rates of 75 megabits per second. There is also a delay of less than five milliseconds before the data transfer starts. The IP-based network architecture of this technology enables smooth voice and data handoff to cell towers of an older generation. Average download and upload speeds for LTE are 77.8 Mbps and 26.9 Mbps, respectively [25, 26].

    - **LTE-A:** By adding a unique physical (PHY) layer and reforming the core network (CN), 3GPP Long-Term Evolution-Advanced (LTE-A) offers significant enhancements over prior mobile network technologies, such as the Universal Mobile Telecommunications System (UMTS) and High-Speed Packet Access (HSPA) [27]. The Long-Term Evolution (LTE) standard is further enhanced by the LTE Advanced standard. Up to three gigabytes of data can be downloaded per second and 1.5 gigabytes of data can be uploaded per second with LTE-Advanced. In contrast, LTE offers 300 Mbps for downloads and 75 Mbps for uploads per second. New transmission protocols and multiple-antenna methods included in LTE-Advanced allow for more bits per bit data transfer, faster handoffs between various cell zones,

and increased data throughput at the level of cell edges and more bits per second into each hertz of spectrum. As a result, the possible outcomes are higher network capacity, more reliable connections, and less expensive data [25, 28].

- **LTE-A Pro:** This is a 3GPP release 13, also referred to as LTE-Advanced Pro. This network technology offered 4.9G, 4.5G Pro, 4.5G, and Pre-5G networks. Long Term Evolution (LTE) has evolved into the LTE-A Pro, which can operate at Gbps. This release included a number of new technologies, including as Massive MIMO, 256 Quadrature Amplitude Modulation, LTE-Unlicensed, and LTE Internet of Things, that may be used in the 5G network system standard. Together with new and developing use cases, this technology offers a wide range of improvements to the problems in the services that are now in place. Furthermore, improvements to Machine-Type-Communication (MTC), improvements to carrier aggregation, improvements to Narrowband-IoT Low Power Wide Area (NB-IoT LPWA), features for public safety, integration with Wi-Fi, single cell-point to multi-point connectivity, licensed assisted access, 3D/FD-MIMO, indoor positioning, and work on latency reduction are among the major advancements made possible by Release 13 [29, 30].

- **5G:** 5G stands for fifth generation wireless system. It is still on the LTE road, but due to a sharp rise in mobile user demand, 4G networks will quickly transition to 5G thanks to cutting-edge access technologies like Filter Bank multi carrier (FBMC) multiple access and Beam Division Multiple Access (BDMA). The idea behind the BDMA technology is that it can support several mobile users at once. This mechanism divides the antenna beam according to the position of the mobile stations in order to provide various access points to the base stations. An orthogonal beam distributes resources to each mobile based station. The capacity of fifth generation wireless mobile networks has increased as a result of this. Massive mobile user connections to base stations are made possible by the 5G standard, which seeks to deliver a larger capacity than 4G networks while also improving the network system. It also performs dependable, dense machine-to-machine communications. High data rates—tens of megabits per second for tens of thousands of users, hundred megabits per second for metropolitan area networks, one gigabit per second for multiple mobile users on a single connection point, and hundreds of thousands of simultaneous connections for wireless network sensors—are among the features of 5G [27, 30]. Only the 1 to 6 GHz spectrum used by LTE is currently available, but for mobile network services utilizing both LTE and 5G technologies, it varies from 1 to 100 GHZ to serve various applications.

3. **Bluetooth and BLE (Bluetooth Low Energy): IEEE 802.15.1 WPAN/Bluetooth:** The IEEE 802.15.1 standard describes how WPAN works. The Bluetooth Special Interest Group's technology serves as the foundation for this standard. WPANs transfer data across small distances without a large infrastructure—in some cases, none at all—or an internet connection. Despite the fact that IEEE 802.15.1 and IEEE 802.11 devices cannot communicate with one another, certain procedures have been devised to enable the coexistence of the two technologies [31]. Using a shared clock, a collection of devices sharing a physical radio channel are synced. Among the devices, one serves as the master, and the others as the slaves. We refer to this topology as piconet. It makes use of a frequency hop transceiver to prevent interference. In order to prevent interference with

static systems, certain frequencies that are available for the hopping pattern are banned. A protocol for low power consumption short-range wireless communications is IEEE 802.15.1 [32]. It was intended to take the position of wired computer accessories with wireless counterparts. Piconet and scatternet are the two topologies that Bluetooth can use. As mentioned above, the piconet topology. Multiple piconets that overlap in space and time make up a scatternet. A device can be proficient in only one piconet, even though it can be a part of multiple ones at once. Despite the possibility of devices being in standby, a piconet can have up to 7 slaves [33]. There are 255 slaves that can be placed in park mode. Up to 20 distinct piconets can be built within a 10-meter radius. Only one packet at a time can be transmitted between slave and master. The cheap cost, mobility, and dynamic network join/leave capabilities of IEEE 802.15.1 are its benefits [34]. Lower data rates, more power consumption, security risks, and less dependability are some of the drawbacks. The proprietary implementation of this standard is called Bluetooth. The issues with versions 1.0 and 1.1 were severe. In 2002, IEEE 802.15.1, version 1.1, was approved [35]. Bluetooth 1.2 has a maximum data transfer rate of 751 kb/s and adds Adaptive Frequency Hopping (AFH) to the previous version. The IEEE 802.15.1-2005 standard was created using it. With Bluetooth 2.0 (2004), the data rate was increased to 2.1 Mbps. Secure Simple Pairing (SSP) was introduced with Bluetooth 2.1 (2007). In the low-power mode, it uses a sniff sub rating to cut down on power usage. The 2009 release of Bluetooth 3.0 increased data transfer rates to 24 Mbps. Bluetooth 4.0 (2010) enhances security and data transfer speeds. There is a significant decrease in power usage. The network topology is the star topology because it prevents devices from being slave devices in many piconets [36]. A slave is permitted to be connected to multiple piconets simultaneously in Bluetooth 4.1 (2013). Additionally, the gadget can switch between the roles of master and slave at different times. The topological options increase as a result. Throughput, security, and internet connectivity have all been enhanced with Bluetooth 4.2 (2014). Lastly, data rate and advertising channel capability are enhanced in Bluetooth 5.0 (2016) range.

4. **LoRa (Long Range):** Long Range, or LoRa, is the name of a proprietary technology developed in 1940. This spread modulation technique makes use of the unlicensed region below 1 GHz. Its long-range transmissions, resilience to interference, and inexpensive cost are its benefits. It is utilized in Internet of Things solutions [37, 38]. The signal in the SUB-GHz ISM band is modulated by the physical layer of LoRa. It employs a spread spectrum method that is exclusive to Semtech Corporation. Numerous benefits are offered by the LoRa network design. LoRa uses the ISM band from 868MHz to 915MHz. With a coverage range of roughly 5 km in cities and 15 km in suburbs, this band is fairly broad. Because of its network architecture and gateway's ability to support thousands of end devices, LoRa is therefore simple to implement. With 125 KHz of bandwidth, the data rate transmission can range from 0.3 Kbps to 27 Kbps. Applications for M2M and IoT use it extensively. As a result, LoRa modulation shares characteristics with FSK modulation, such as constant envelope modulation. LoRa technology is inexpensive and offers high efficiency at minimal power.

5. **Z-Wave:** Although it may not be a name you hear often, "Z-wave" (Z-Wave Alliance ZAD12837 / ITU-T G.9959) is quickly becoming one of the most widely used wireless technologies for Internet of Things devices. Z-wave is a unique protocol designed primarily for home automation and networking. Right now, Amazon's Echo is arguably the most well-known example of Z-wave technology, having completely changed how tech-savvy customers consume media and shop. More than 2000 Z-wave products are available on the market, enabling connectivity for a variety of home appliances, including thermostats, fans, blinds, fire alarms, and smart garage door openers. Z-wave systems function in the frequency spectrum below 1 GHz and typically have a range of up to 30 meters.

Table 1: Strengths and Weaknesses of Each Wireless Technology

Characteristics	**Wi-Fi (IEEE 802.11)**	**Bluetooth**	**Zigbee**	**Mobile Networks (4G LTE and 5G)**	**Z-Wave**	**LoRa (Long Range)**
Power Consumption	Moderate to High, especially during data transmission	Low to Moderate, especially in Bluetooth Low Energy (BLE) versions.	Low, especially in low-power sleep modes.	Moderate to High, especially during data-intensive activities.	Low to Moderate, especially in low-power sleep modes.	Low, especially in low-power, wide-area networks.
Range	Moderate to High, typically within a hundred meters	Short to Moderate, typically within tens of meters.	Short to Moderate, typically within tens of meters.	Long, providing wide-area coverage.	short to Moderate, typically within tens of meters.	Long, typically several kilometers.
Scalability	Good scalability, suitable for environments with a large number of devices.	Moderate scalability, suitable for personal area networks and applications with a moderate number of devices.	High scalability, suitable for large-scale sensor networks and home automation.	High scalability, suitable for wide-scale deployments.	High scalability, suitable for home automation and smart building applications.	High scalability, suitable for large-scale deployments covering extensive areas.
Data Rates	Up to several Gbps (Wi-Fi 6)	Up to 2 Mbps (Bluetooth 5.0)	Up to 250 kbps	Up to several hundred Mbps (4G LTE), potentially several Gbps (5G)	Up to 100 kbps	Typically ranges from 0.3 kbps to 50 kbps, depending on spreading factor and modulation

Suitability	Well-suited for applications with higher data rates, such as video streaming, and in environments with reliable power sources	Ideal for low-power, short-range applications such as wearables, health monitoring, and smart home devices.	Well-suited for low-power, low-data-rate applications in home automation, industrial automation, and smart lighting	Ideal for applications requiring high data rates, mobility, and connectivity over long distances, such as smart cities and mobile IoT devices	Well-suited for low-power, low-data-rate applications in smart home and building automation.	Ideal for low-power, long-range applications such as smart agriculture, environmental

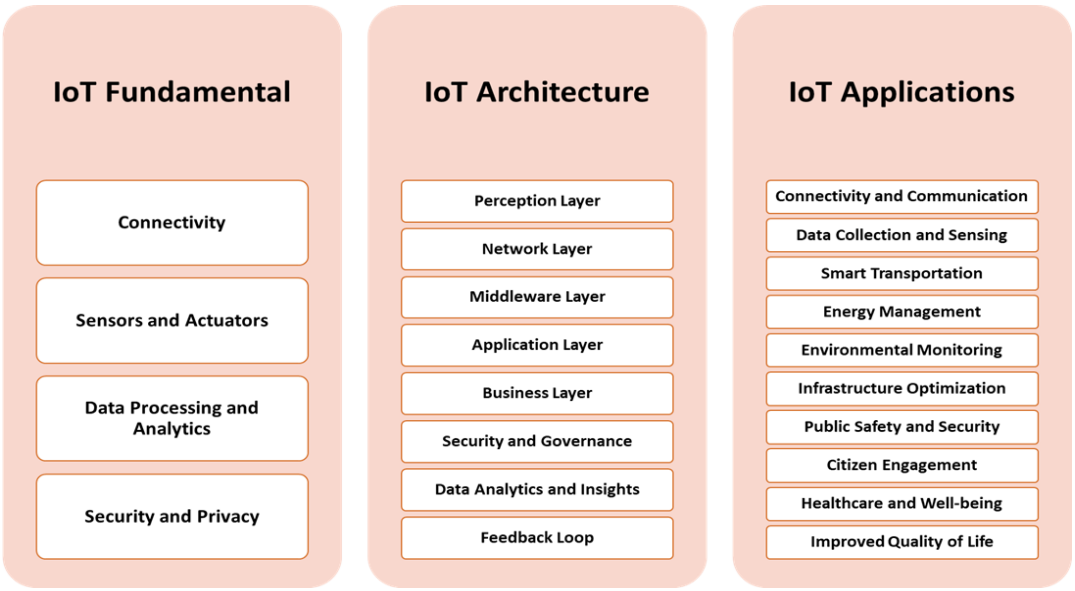

Figure 5: IoT Fundamentals, its Architecture and Applications

III. IOT FUNDAMENTALS AND ARCHITECTURE IN SMART CITIES

In the development of a smart city, the Internet of Things (IoT) behaves as a technological backbone that enables the seamless integration of diverse devices, systems, and services to enhance the life of urban citizens. The study of fundamentals and architecture of IoT is necessary to understand the basic functioning of IoT and its role in the formation of the smart cities in urban planning. Figure 5 shows the IoT fundamentals, its architecture and applications.

1. IoT Fundamentals

- **Connectivity:** IoT devices depend on various wireless technologies, such as WiFi, Bluetooth, Zigbee, and cellular networks, for connectivity. To accommodate battery-operated devices, low-power communication protocols like MQTT and CoAP are commonly used.

- **Sensors and Actuators:** IoT employs a network of sensors to collect data on environmental conditions, traffic flow, energy consumption, and more. These sensors collect the data from the physical world. The actuators are the devices that are capable of performing actions based on data received, such as adjusting streetlights or controlling irrigation systems.

- **Data Processing and Analytics:** Once the data is collected, it is processed at the edge of the network to reduces latency and enable real-time decision-making.This is called Edge Computing. With the help of cloud computing for which the centralized cloud platforms are utilized, the data is stored and complex analytics, and machine learning applications.

- **Security and Privacy:** To secure the data during transmission and storage the encryption on the data is performed. Authentication is another important aspect so as to verify the identity of devices and users within the IoT ecosystem. To ensure the protection of personal and sensitive data various privacy measures are considered.

2. IoT Architecture in Smart Cities

- **Perception Layer:** The function of the Perception Layer is to collect data from the physical environment and perform actions based on the received information. Within the domain of this layer, the gateways and edge computing devices process and filter data before transmission.

- **Network Layer:** This is the next layer in the ToT architecture after the Perception Layer. It is responsible for providing Connectivity through wireless networks facilitating communication between devices. For this the standardized set of communication protocols ensure interoperability. Protocols like MQTT and CoAP are commonly used. Interconnected devices create robust mesh networks for improved coverage.

- **Middleware Layer:** The middleware Layer processes and manages data, transforming raw sensor data into actionable insights. It allows device management by encompassing tasks such as provisioning, configuring, and updating IoT devices.

- **Application Layer:** This layer offers smart city applications for which a large number of the implementations are there varying from traffic management and waste monitoring to healthcare and public safety. It also provides the user interfaces where the dashboards and applications provide users with real-time information and control over connected services.

- **Business Layer:** This layer handles the integration with urban planning by aligning IoT implementations with city planning goals. For the monetization modeling it explores business models for sustainable IoT deployments in smart cities.

- **Security and Governance:** This layer facilitates access control by regulating access to devices and data. The blockchain technology is incorporated to ensure secure, transparent, and tamper-proof transactions. It also adheres to data protection and privacy regulations.

- **Data Analytics and Insights:** For the data analytics the layer offers big data analysis by processing large volumes of data for trend analysis and pattern recognition. The layer is also responsible for predictive modeling in which the forecasting of the future events is based on historical data.

- **Feedback Loop:** It has the closed-loop systems where feedback from IoT applications leads to dynamic adjustments and improvements. In order to seek continuous improvement, iterative processes for refining and optimizing smart city solutions is followed.

IV. IOT APPLICATIONS IN URBAN PLANNING

1. **Connectivity and Communication:** Wireless technologies, such as Wi-Fi, Zigbee, and LoRa, enable seamless connectivity among a myriad of IoT devices spread across a city. It also offers real-time communication where wireless communication protocols facilitate real-time data exchange between sensors, devices, and central systems.

2. **Data Collection and Sensing:** Wireless-enabled sensors gather data on various urban parameters, including air quality, traffic flow, energy consumption, and more. The wireless networks not only provide a wide coverage but with the flexibility to deploy sensors over a large geographical area, covering diverse aspects of urban life.

3. **Smart Transportation:** Wireless technologies support intelligent transportation systems (ITS) that enhance traffic flow and reduce congestion. Wireless communication between vehicles and infrastructure ensures that the traffic optimization is achieved with safety.

4. **Energy Management:** The smart grids are used for wireless networks to facilitate communication between devices ensuring energy optimization, distribution and consumption. Wireless technologies allow remote monitoring and control of energy infrastructure, contributing to efficiency and sustainability.

5. **Environmental Monitoring:** Wireless sensor networks are exploited to monitor environmental parameters such as air and water quality, noise levels, and temperature. For environmental hazards, the early warning systems provide rapid data transmission.

6. **Infrastructure Optimization:** Wireless connectivity in IoT for smart cities and urban planning, allows for real-time monitoring of critical infrastructure, such as bridges, buildings, and utilities. It also offers predictive maintenance by acquiring the data from IoT sensors enabling reduced downtime and improved infrastructure resilience.

7. **Public Safety and Security:** Wireless technologies support surveillance cameras and IoT-enabled security systems for public safety. Along with this the emergency response facility caters to real-time data transmission to enhance emergency services to aid crisis management.

8. **Citizen Engagement:** Wireless connectivity enables citizens to engage through mobile applications for reporting issues, accessing services, and providing feedback. Community Participation: Wireless technologies foster citizen involvement in urban planning and decision-making processes.

9. **Healthcare and Well-being:** Wireless IoT applications contribute to remote healthcare monitoring and emergency response systems. Apart from this it enables wearable devices with wireless connectivity to collect health data, contributing to personalized well-being services.

10. **Improved Quality of Life:**Wireless technologies optimize service delivery, contributing to a more efficient and livable urban environment. Overall, wireless-enabled IoT applications enhance the quality of life for residents by improving services, sustainability, and resource management. In essence, wireless technologies form the backbone of IoT in smart cities, enabling the continuous flow of data and communication needed for intelligent decision-making, efficient resource management, and the creation of more sustainable and livable urban spaces.

V. CHALLENGES IN IMPLEMENTATION WITH RESPECTIVE MITIGATIONS

The implementation of IoT (Internet of Things) in smart cities and urban planning comes with various challenges that need to be addressed to ensure a successful and secure deployment. Some of the key challenges include:

1. **Scalability Issues:** With the increment and growth of IoT devices, managing and scaling the infrastructure becomes a significant challenge. It may result in the poor handling of a growing number of devices and may lead in performance degradation and reduced system responsiveness. To mitigate this challenge, the robust architecture design, use of scalable cloud platforms, and optimization of communication protocols can be exploited.

2. **Security Concerns:** The IoT devices are vulnerable to security threats, including unauthorized access, data breaches, and malicious attacks. This may lead to security breaches with compromised data integrity, privacy violations, and disruptions in critical services. By implementing robust encryption, authentication mechanisms, regular security audits, and keeping devices and software up-to-date can enhance security and mitigate these issues.

3. **Interoperability Challenges:** IoT ecosystems largely consist of devices from various manufacturers using different communication protocols and standards, leading to interoperability challenges. Here the possible implication could hinder seamless communication and integration of devices leading to limited effectiveness of the IoT system. To mitigate this challenge, the adoption of common standards, development

of interoperability frameworks, and collaboration between industry stakeholders can be useful.

4. **Data Privacy and Ethics:** Now a-days a bulk of personal data is available on the cloud. Therefore, the collection, storing, and processing of vast amounts of data from IoT devices raise concerns about individual's privacy and the ethical use of data. As a consequence of it there is a huge possibility of mishandling of sensitive data that can erode public trust and lead to legal and regulatory challenges. In order to handle this implementation, privacy-by-design principles, transparent data handling practices, and adherence to data protection regulations can be done.

5. **Reliability and Resilience:** IoT systems must be reliable and resilient to handle disruptions, outages, or failures in devices or network connectivity. Any unreliability of the systems can result in service interruptions and can negatively impact critical applications. To handle this problem the redundancy, failover mechanisms, and proactive maintenance can be trusted.

6. **Power Consumption and Battery Life:** Many of the IoT devices operate on battery power, and optimizing energy consumption is crucial for extended battery life. The short battery life can lead to frequent replacements and increased maintenance costs. In order to overcome this problem, the low-power design, energy-efficient communication protocols, and the use of energy harvesting technologies can be utilized.

7. **Cost Considerations:** The initial deployment and ongoing maintenance costs of IoT infrastructure can be significant. So the budget constraints may hinder the widespread adoption of IoT solutions in smart cities. The possible mitigation techniques could be cost-benefit analyses, public-private partnerships, and gradual, phased deployments.

8. **Regulatory and Compliance Issues:** Compliance with various regulations and standards, especially in areas like data protection, can pose challenges. Therefore, the non-compliance may lead to legal issues and hinder the acceptance of IoT solutions. Thorough understanding of regulatory requirements, proactive compliance measures, and engagement with regulatory authorities, the regulatory challenges can be addressed.

9. **Lack of Skill Sets:** The complexity of IoT systems requires skilled professionals for design, implementation, and maintenance. So, the shortages in skilled personnel can lead to challenges in effectively managing IoT deployments. In order to meet the challenges, the training programs, educational initiatives, and collaboration with academic institutions are helpful to build a skilled workforce. Addressing these challenges requires a multi-faceted approach involving technology, policy, and collaboration among stakeholders. By proactively addressing scalability, security, interoperability, and other challenges, smart cities can maximize the benefits of IoT for improved urban living.

VI. ADVANCED SOLUTIONS AND INNOVATIONS

To overcome the challenges in implementing IoT in smart cities and urban planning, various solutions and innovations have been developed. Here are some key advancements in security measures, interoperability standards, and computing paradigms like edge computing and fog computing:

1. **Security Concerns:** These concerns can be addressed by the three advanced solutions that are, blockchain technology, zero trust architecture and AI-driven security analytics. The integration of blockchain for secure and transparent transactions ensures data integrity and prevents unauthorized access. The zero trust architecture adopts a zero-trust model, where devices and users are continuously authenticated and verified to enhance overall security. The AI-driven security analytics utilizes artificial intelligence to analyze patterns and anomalies in real-time, identifying potential security threats.

2. **Interoperability Challenges:** The interoperability challenges are addressed by techniques such as open standards and protocols, IoT platforms and industry alliances. The open standards and protocols increase adoption of open standards and communication protocols to enhance interoperability among diverse IoT devices. The IoT platforms offer the development of comprehensive IoT platforms that provide a common framework for integrating and managing diverse devices and applications. Finally, the industry alliances cater to the collaboration among industry stakeholders to establish common standards and ensure compatibility across different IoT ecosystems.

3. **Edge Computing:** For edge computing, three major techniques are deployed that include distributed edge architecture, edge analytics and edge security. The distributed edge architecture technique pushes the processing closer to the data source, reducing latency and enhancing real-time decision-making. The edge analytics performs data analytics at the edge to filter and process relevant information locally, minimizing the need for extensive data transfer. The edge security is used to implement security measures directly at the edge to protect data at its source.

4. **Data Privacy and Ethics:** Data privacy and ethics use homomorphic encryption and differential privacy approaches. The homomorphic encryption allows computations on encrypted data without decrypting it, ensuring privacy in data processing while the differential privacy technique introduces noise to individual data points to protect user privacy while still allowing aggregate analysis.

5. **Fog Computing:** To accomplish the fog computing technique, various new approaches are adopted such as fog-to-cloud continuum, proximity-based services and resource orchestration. The fog-to-cloud continuum combines fog computing (distributed edge computing) with cloud resources to create a continuum for data processing and storage. In proximity-based services the utilization of fog computing is there to provide location-based and context-aware services, enhancing user experiences. In the third technique which is the resource orchestration, the dynamic allocation of computing resources across fog and cloud layers based on workload demands is done.

6. **Secure Device Onboarding:** The secure device onboarding is done by using different techniques such as device identity management and device authentication are exercised. The device identity management is used to implement robust identity management for IoT devices to ensure secure onboarding while device authentication offers leveraging advanced authentication mechanisms, including biometrics and multi-factor authentication, to enhance device security.

7. **AI-driven Threat Detection:** The AI-driven threat detection can be done by behavioral analytics where the machine learning algorithms are used to analyze and identify abnormal behavior patterns, helping detect security threats. The other way to resolve this issue is the anomaly detection in which the AI-driven anomaly detection is employed to identify deviations from normal behavior and potential security breaches.

8. **Self-Healing Systems:** The Self-Healing Systems include autonomous security measures by implementing self-healing capabilities in IoT systems to automatically respond to and mitigate security threats. The self healing can also be catered by using predictive maintenance which uses AI and machine learning to predict potential security vulnerabilities.

9. **Standardized Data Models:** The standardized data models include semantic interoperability and data description standards. The semantic interoperability establishes standardized data models and semantic interoperability to ensure consistent and meaningful communication among diverse devices on the other hand the data description standards defines standardized metadata and descriptions for IoT data to enhance understanding and compatibility.

10. **Edge-to-Cloud Integration:** The edge-to-cloud integration technology includes seamless data flow and hybrid architectures. The seamless data flow ensures smooth integration and data flow between edge devices and cloud platforms at the same time the hybrid architecture technique implements hybrid architectures that balance computing tasks between edge and cloud resources based on specific requirements.

11. **Regulatory Compliance Frameworks:** For the regulatory compliance and frameworks the adopted methodologies are adherence to standards that develop and adhere to regulatory frameworks and standards to ensure compliance with data protection and privacy regulations. The other method in this regard is transparency and accountability which establishes transparent practices and mechanisms for accountability in handling and securing IoT data.

12. **Dynamic Resource Allocation:** The dynamic resource allocation includes resource-efficient algorithms that develop algorithms that dynamically allocate resources based on real-time demand, optimizing computing resources and energy consumption. The other approach is load balancing that implements effective load balancing mechanisms for distributed computing environments.

13. **Secure Device Lifecycle Management:** To achieve the secure device lifecycle management, an end-to-end Security mechanism is deployed that ensures security measures throughout the entire lifecycle of IoT devices, including manufacturing,

deployment, and decommissioning. The device firmware updates are the other technique that implements secure mechanisms for updating device firmware to patch vulnerabilities and enhance security. Advancements in these areas contribute to building a more secure, interoperable, and efficient IoT ecosystem for smart cities and urban planning. Continuous innovation and collaboration among industry stakeholders are essential to addressing the evolving challenges and ensuring the sustainable growth of IoT in urban environments.

VII. FUTURE TRENDS AND DEVELOPMENTS

The future of IoT in smart cities and urban planning is poised for continued growth and innovation, driven by advancements in technology, evolving urban challenges, and the increasing demand for smarter, more sustainable cities. Several trends and developments are expected to shape the future landscape of IoT in urban environments that is shown in Fig.6:

1. **5G Integration:** The rollout of 5G networks will significantly enhance connectivity, enabling faster data transfer, lower latency, and support for a massive number of devices. Accelerated adoption of IoT applications in smart cities, especially those requiring real-time communication and high data throughput.

2. **Edge Computing Maturity:** Edge computing will mature, becoming more widespread and sophisticated, allowing for more processing at the edge of the network. Improved real-time decision-making, reduced latency, and enhanced overall system efficiency in IoT deployments.

Figure 6: Future Trends of IoT in Smart Cities and Urban Planning

3. **AI and Machine Learning Integration:** Increasing integration of AI and machine learning into IoT systems for advanced analytics, predictive modeling, and automation. Smarter and more adaptive systems capable of learning and evolving, leading to improved resource optimization and decision-making.

4. **Digital Twins for Urban Planning:** The use of digital twins—virtual replicas of physical assets or systems—for comprehensive urban planning and simulation. Enhanced visualization, monitoring, and predictive modeling for urban infrastructure, enabling more informed decision-making.

5. **Autonomous Vehicles and Traffic Management:** Advancements in autonomous vehicle technology and intelligent traffic management systems for safer, more efficient urban mobility. Reduced traffic congestion, improved transportation efficiency, and enhanced safety through automated and connected vehicle systems.

6. **Smart Health and Well-being Solutions:** Expansion of IoT applications in healthcare, including remote patient monitoring, wearable devices, and smart health infrastructure. Improved healthcare accessibility, personalized medicine, and enhanced public health monitoring.

7. **Blockchain for Security and Trust:** Increased adoption of blockchain technology for enhancing security, data integrity, and trust in IoT ecosystems. Strengthened security measures, transparent transactions, and improved trust among stakeholders in smart city environments.

8. **Sustainable and Resilient Infrastructure:** Growing emphasis on IoT solutions for sustainable and resilient urban infrastructure, addressing environmental challenges and climate change. Implementation of IoT-driven solutions for energy efficiency, waste reduction, and sustainable urban development.

9. **Augmented Reality (AR) in Urban Services:** Integration of augmented reality technologies for enhanced citizen engagement, navigation, and interactive urban services. Improved user experiences, increased civic participation, and more intuitive interaction with smart city services.

10. **Privacy-Preserving Technologies:** Continued development and adoption of privacy-preserving technologies, such as homomorphic encryption and federated learning. Enhanced protection of user privacy while still allowing for valuable data analysis and insights.

11. **Quantum Computing Impacts:** Exploring the potential impacts of quantum computing on IoT applications, particularly in solving complex problems and optimizing algorithms. Accelerated data processing, improved encryption methods, and advancements in optimization algorithms.

12. **Resilience in the Face of Disasters:** IoT solutions designed to enhance urban resilience and response during natural disasters and emergencies. Improved early warning systems, efficient evacuation planning, and enhanced disaster response and recovery.

13. **Human-Centric Design:** Emphasis on human-centric design principles to ensure that IoT applications prioritize user experiences, inclusivity, and accessibility. More user-friendly and inclusive smart city solutions that cater to diverse needs and demographics.

14. **Regulatory Frameworks and Governance:** Development of robust regulatory frameworks and governance models to address ethical considerations, data privacy, and security in smart city deployments. Clearer guidelines, increased trust, and responsible implementation of IoT technologies in urban environments. The future trends in IoT for smart cities reflect a dynamic landscape where technology continues to evolve, and cities strive to become more connected, efficient, and sustainable. As these trends unfold, collaboration among stakeholders, regulatory frameworks, and a focus on ethical considerations will play crucial roles in shaping the successful and responsible implementation of IoT in urban environments.

VIII. CONCLUSION

The chapter on wireless technologies in IoT and urban planning explores the pivotal role that wireless communication plays in shaping the future of smart cities. The integration of wireless technologies within the Internet of Things (IoT) framework presents a transformative approach to urban planning, enhancing connectivity, efficiency, and the overall quality of life for city residents. The purpose of this chapter was to cover wireless technologies exploited in IoT and urban planning along with the comparison of each technology's strengths and weaknesses. The IoT fundamentals and architecture in smart cities are considered with the focus on the IoT applications in urban Planning. It included awareness of the challenges of implementing wireless IoT in urban environments along with the practical solutions and strategies to address these challenges. It also focused on an overview of future trends and finally the conclusion of the work.

REFERENCES

[1] G. Baldini, S. Karanasios, D. Allen, and F. Vergari, "Survey of wireless communication technologies for public safety," *IEEE Commun. Surv. Tutorials*, vol. 16, no. 2, pp. 619–641, 2014, doi: 10.1109/SURV.2013.082713.00034.

[2] Aliouat, N. Kouadria, S. Harize, and M. Maimour, "An Efficient Low Complexity Region-of-Interest Detection for Video Coding in Wireless Visual Surveillance," *IEEE Access*, vol. 11, no. January, pp. 26793–26806, 2023, doi: 10.1109/ACCESS.2023.3248067.

[3] S. Tanwar, S. Tyagi, and S. Kumar, "The Role of Internet of Things and Smart Grid for the Development of a Smart City," *Lect. Notes Networks Syst.*, vol. 19, no. September, pp. 23–33, 2018, doi: 10.1007/978-981-10-5523-2_3.

[4] "J2ME-BASED WIRELESS INTELLIGENT VIDEO SURVEILLANCE SYSTEM USING MOVING OBJECT RECOGNITION," *Int. J. Multidiscip. Eng. Curr. Res.*, vol. 8, no. 10, 2023.

[5] L. Garcia, J. M. Jiménez, M. Taha, and J. Lloret, "Wireless Technologies for IoT in Smart Cities," *Netw. Protoc. Algorithms*, vol. 10, no. 1, p. 23, 2018, doi: 10.5296/npa.v10i1.12798.

[6] F. P. ERINA FERRO and ISTI, "Bluetooth and Wi-Fi Wireless Protocols :," *IEEE Wirel. Commun.*, pp. 1–24, 2004.

[7] D. Kim, Y. Yoon, J. Lee, P. J. Mago, K. Lee, and H. Cho, "Design and Implementation of Smart Buildings: A Review of Current Research Trend," *Energies*, vol. 15, no. 12, 2022, doi: 10.3390/en15124278.

[8] Triantafyllou, P. Sarigiannidis, and T. D. Lagkas, "Network protocols, schemes, and mechanisms for internet of things (IoT): Features, open challenges, and trends," *Wirel. Commun. Mob. Comput.*, vol. 2018, 2018, doi: 10.1155/2018/5349894.

[9] Wang *et al.*, "Artificial Intelligence Enabled Wireless Networking for 5G and Beyond : Recent Advances and Future Challenges Artificial Intelligence Enabled Wireless Networking for 5G and Beyond : Recent Advances and Future Challenges," *IEEE Wirel. Commun.*, vol. 27, no. 1, pp. 16–23, 2020.

[10] M. Chen, U. Challita, W. Saad, and C. Yin, "Machine Learning for Wireless Networks with Artificial Intelligence : A Tutorial Machine Learning for Wireless Networks with Artificial Intelligence : A Tutorial on Neural Networks," no. October, 2017.
[11] D. Jiang, "The construction of smart city information system based on the Internet of Things and cloud computing," *Comput. Commun.*, vol. 150, pp. 158–166, 2020, doi: 10.1016/j.comcom.2019.10.035.
[12] Ahmad, S. Shahabuddin, T. Kumar, E. Harjula, M. Meisel, and M. Juntti, "Challenges of AI in Wireless Networks for IoT," *IEEE Ind. Electron. Mag.*, no. April, 2020, doi: 10.1109/MIE.2020.2979272.
[13] S. Stephenson, "Abuse Vectors : A Framework for Conceptualizing IoT-Enabled Interpersonal Abuse," 2023.
[14] N. A. Zaimy, M. F. Zolkipli, and N. Katuk, "A review of hacking techniques in IoT systems and future trends of hacking on IoT environment," *World J. Adv. Res. Rev.*, vol. 17, no. 02, pp. 723–731, 2023.
[15] H. Azam *et al.*, "Wireless Technology Security and Wireless Technology Security and Privacy : A Comprehensive Study," 2023, doi: 10.20944/preprints202311.0664.v1.
[16] T. Shanthi, M. S. Sheela, J. J. Jayakanth, M. Karpagam, G. Srividhya, and T. V. S. Gowtham Prasad, "A Novel approach Secure Routing in Wireless Sensor Networks for Safe Path Establishment of Private IoT Data Transmission," *Int. J. Intell. Syst. Appl. Eng.*, vol. 11, no. 9s, pp. 455–460, 2023.
[17] S. R. Rajeswari and V. Seenivasagam, "Comparative Study on Various Authentication Protocols in Wireless Sensor Networks," *Sci. World J.*, vol. 2016, no. iii, 2016, doi: 10.1155/2016/6854303.
[18] Y. Zheng, G. Zhang, Z. Huan, Y. Zhang, and G. Yuan, "Space Solar Power and Wireless Transmission Wireless laser power transmission : Recent progress and future challenges," *Sp. Sol. Power Wirel. Transm.*, no. June 2023, 2024, doi: 10.1016/j.sspwt.2023.12.001.
[19] H. K. 3 and R. K. Mohammed H. Alsharif 1,* , Abu Jahid 2,*, "SS symmetry Green IoT : A Review and Future Research Directions," *Symmetry (Basel).*, vol. 15, no. 757, pp. 1–37, 2024
[20] Yaqoob, I. Abaker, T. Hashem, Y. Mehmood, A. Gani, S. Mokhtar and S. Guizani, "Enabling Communication Technologies for Smart Cities", IEEE Communications Magazine, January 2017, pp. 112-120. DOI: https://doi.org/ 10.1109/MCOM.2017.1600232CM
[21] S. Sendra, M. Garcia, C. Turro and J. Lloret, "WLAN IEEE 802.11 a/b/g/n Indoor Coverage and Interference Performance Study", International Journal on Advances in Networks and Services, Vol. 4, no 1, pp. 209-222, 2011. DOI: https://doi.org/ 10.1109/ICWMC.2010.46
[22] S. Sendra, P. Fernandez, C. Turro and J. Lloret, "IEEE 802.11 a/b/g/n Indoor Coverage and Performance Comparison", The Sixth International Conference on Wireless and Mobile Communications. ICWMC 2010, Valencia, Spain, 20-25 September 2010, pp. 185-190. DOI: https://doi.org/ 10.1109/ICWMC.2010.46
[23] S. C. Ergen, "ZigBee/IEEE 802.15.4 Summary", UC Berkeley, Vol. 10, September 2004, pp. 17.
[24] K. Mikhaylov, N. Plevritakis and J. Tervonen, "Performance Analyss and Comparison of Bluetooth Low Energy with IEEE 802.15.4 and SimpliciTI", Journal of Sensor and Actuator Networks, Vol. 2, no 3, August 2013, pp. 589-613. DOI: https://doi.org/ 10.3390/jsan2030589
[25] E. Dahlman, S. Parkvall and J. Skold, "4G: LTE/LTE-Advanced for Mobile Broadband", 1st Edition, Academic press, 2013
[26] W. Jung and Y. Kwon, "Differences between LTE and 3G service customers: Business and policy implication" , Telematics and Informatics, Vol. 32, no. 4, pp. 667-680, 2015. DOI: https://doi.org/ 10.1016/j.tele.2015.03.001
[27] E. Kammoun, F. Zarai, and M.S. Obaidat "Chapter 6 – LTE and 5G systems", Smart Cities and Homes, Key Enabling Technologies, pp. 111–129, 2016. DOI: https://doi.org/10.1016/B978-0-12-803454-5.00006-7
[28] S. Ahmadi, "LTE-Advanced: a practical systems approach to understanding 3GPP LTE releases 10 and 11 radio access technologies", Academic Press, 2013.
[29] H. Ji, Y. Kim, J. Lee, E. Onggosanusi, Y. Nam, J. Zhang, B. Lee and B. Shim, "Overview of full-dimension MIMO in LTE-advanced pro", IEEE Communications Magazine, Vol. 55, No. 2, pp.176-184, 2016.
[30] Haidine, and S. El Hassani, "LTE-a pro (4.5 G) as pre-phase for 5G deployment: closing the gap between technical requirements and network performance", International Conference on Advanced Communication Systems and Information Security (ACOSIS), Marrakesh, Morocco, 17-19 October 2016, pp. 1-7. DOI: https://doi.org/10.1109/ACOSIS.2016.7843933
[31] IEEE Computer Society, "Part 15.1: Wireless medium access control (MAC) and physical layer (PHY) specifications for wireless personal area networks (WPANs)", 14 June 2005
[32] J. Lee, Y. Su and C. Shen, "A Comparative Study of Wireless Protocols: Bluetooth, UWB, ZigBee and WiFi", 33rd Annual Conference of the IEEE Industrial Electronics Society (IECON), Taipei, Taiwan, 5-8 November, 2007, pp. 46-51. DOI: https://doi.org/ 10.1109/IECON.2007.4460126

[33] C. Bisdikian, “An Overview of the Bluetooth Wireless Technology”, IEEE Communications Magazine, Vol. 39, no 12, December 2001, pp 86-94. DOI: https://doi.org/ 10.1109/35.968817
[34] E. Ferro and F. Potortì, “Bluetooth and Wi-Fi wireless protocols: A survey and comparison”, IEEE Wireless Communications, Vol. 12, no 1, February 2005, pp. 12-26. DOI: https://doi.org/ 10.1109/MWC.2005.1404569
[35] S. Vyas, U. Chaudhari, V. C. Nandini and B. Thakare, “State of the Art Literature Survey 2015 on Bluetooth”, International Journal of Computer Applications, Vol. 131, no 8, December 2015, pp. 7-10. DOI: https://doi.org/ 10.5120/ijca2015907391 [29] S. Darroudi and C. Gomez, “Bluetooth Low Energy Mesh Networks: A Survey”, Sensors, MDPI, Vol. 17, no 7, 22 June 2017, pp. 1467. DOI: https://doi.org/10.3390/s17071467
[36] S. Darroudi and C. Gomez, “Bluetooth Low Energy Mesh Networks: A Survey”, Sensors, MDPI, Vol. 17, no 7, 22 June 2017, pp. 1467. DOI: https://doi.org/10.3390/s17071467
[37] R. S. Sinha, Y. Wei and S. Hwang, “A survey on LPWA technology: LoRa and NB-IoT”, ICT Express, Vol. 3, No. 1, pp. 14-21, March 2017. DOI: https://doi.org/ 10.1016/j.icte.2017.03.004
[38] Augustin, J. Yi, T. Clausen and W. M. Townsley, “A Study of LoRa: Long Range & Los Power Networks for the Internet of Things”, SENSORS, Vol. 16, No. 9, p. 1466, 2016. DOI: https://doi.org/10.3390/s16091466

