Investigation about wireless communications network protocols for smart cities

MUSTAFA K. ATI
Department of Electrical Engineering & college of engineering
University of Misan
IRAQ

Abstract: - There is rapid growth in the number of Internet of Things (IoT) devices both now and in the future; these devices require protocols to connect to a central server. Many protocols have been implemented to facilitate this connection. This paper provides a review of commonly used protocols in the field of IoT for communication devices in smart cities. Through this study, it is found that the Message Queuing Telemetry Transport (MQTT) protocol has many features over the rest protocols, To its simplicity and lightweight, it also supports a wide range of internet of things IoT applications, and it provides the security of Transport Layer Security/Secure Sockets Layer (TLS/SSL) shown in Table 1.

Key-Words: Internet of Things, sensor networks, MQTT protocol, communication layers, Smart cities, IoT devices.

Received: April 5, 2024. Revised: November 29, 2024. Accepted: March 9, 2025. Published: May 19, 2025.

1. Introduction

The development of Industrial IoT (IIoT) is being driven by the acceptance of new technical developments and Internet of Things (IoT) applications in industrial systems. By automating smart things, IIoT offers a fresh take on IoT in the industrial sector. For detecting [1-3]. The Internet of Things (IoT) is defined as a network of physical objects are each interconnected and to each other without requiring human involvement for data transfer or control. Smart linked cars, intelligent logistics, smart homes, and precision agriculture are just a few of the many possible uses for the Internet of Things, etc. [4-6]. It features cutting-edge electronic platform communication technology. The IoT system, which consists of communication, storage, and apps, also includes components for temperature, wind , moisture levels, fire alarms, and burglar alarms. Massive data cellular, Bluetooth, and local area networks, Zigbee and long-range communication. For data storage, you have a choice between a locally hosted database and an online service that provides access to databases and other computer resources on demand The application layer serves as a bridge between the cloud server and the customers who access the final sensor data via web-based or mobile applications [7,8].

2. Wireless Sensor Infrastructure

Looking at many types of studies on IoT embedded systems, it was discovered that there is no widely accepted technique for the Internet of Things; hence, several architectures have been intensively examined[23].

2.1. Three and five Level Paradigms

Three and five layers [3–5] represent the easy architecture of the communication layers. The three-layer architecture, as shown in Figure 1, comprises application network and perception [23].

2.2 . The Application layer (Fog layer)

It identifies physical characteristics or finds intelligent entities in the surroundings and is represented by hardware with devices for sensing and acquiring environmental data, shown in figure 1 [23].

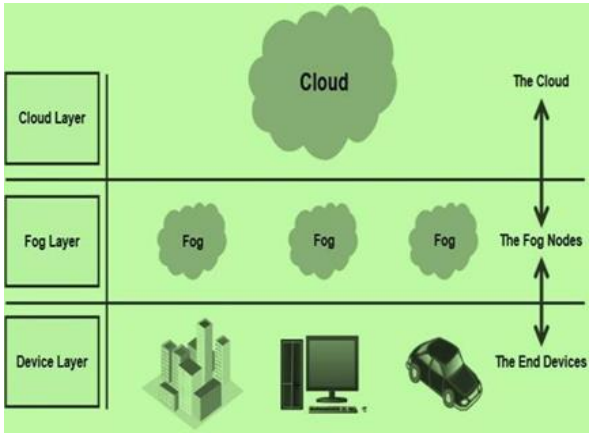

Figure. 1: Architecture of IoT three layers [23].

2.3 . The Network layer (Devices layer)

It is working to connect hosts, network hardware, and bright objects; sensor use is also possible, as is data transmission and processing[3-6].

2.4 . The perception layer

It provides customers with implementation services and defines Internet of Things applications such as smart things, intelligent buildings, and smart device health. Although the three-layer design explains the essential emergence of the Internet of Things, it is frequently unsuitable for IoT research. As a result, the literature suggests many additional layered architectures .Perception, communication, analysis, implementation, and commerce are the tiers (see Figure 1). Crucial parts in the chain of events that leads to a safe connection for the flow of data[3-6].

2.5 . The transport layer

Wi-Fi, Bluetooth, and near-field communication (NFC) networks are utilized by the transport layer in order to send sensor data from the perception layer to the processing layer and vice versa [3-6].

2.6 . The processing layer (cloud layer)

It stores, analyzes, and processes enormous quantities of transport layer data. It has the ability to administrate and service the lower tiers; it is the final decision maker[3-6].

2.7 . The business layer

It's one of the most important layers in communication systems because it monitors things like IoT applications, business economic models, and user privacy[3-6].

2.7.1 Shadow and sensor systems

The cloud is a data center for information transmitted from Internet of Things devices. When signals are sent from these devices, they are processed and responded to by special processes within the cloud-based communications system [9]. For the transmission and reception process to be flexible and fast, these signals must be well encrypted to ensure they reach the user with high accuracy and security. Starting from their transmission via Internet of Things devices, through the smart cloud, and finally reaching the subscriber. This note is very important to ensure smooth, accurate, and secure communication through the use of an advanced and intelligent customer service communication system [24], shown in figure (2).

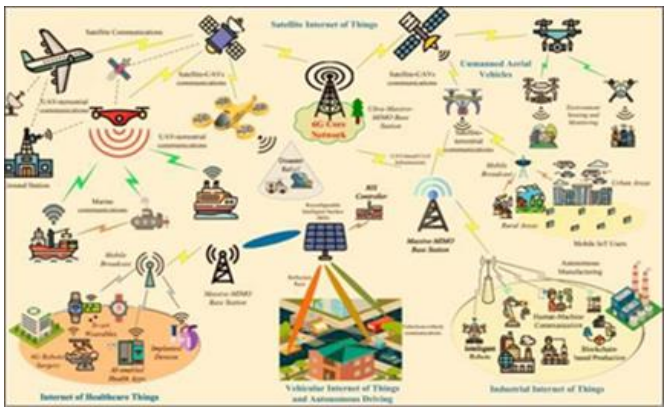

Figure. 2: Smart cities and IoT devices [30]

2.7.2 .Sensing and Actuating Devices

Sensors are necessary for all Internet of Things (IoT) applications in gathering data from their surroundings. For an intelligent item to function, it needs sensors. Sensor technology is essential to the IoT. Because context awareness cannot be achieved without it. Sensors on the Internet of Things (IoT) are often compact, inexpensive, and power-efficient. They're limited by battery capacity and the ease with which they may be deployed. Intelligent applications are built with various sensors, as described by Stein and Of Laerhoven [16].

3 . Internet of Things Protocol Stack

The majority of IoT gadgets use a web as their "active layer." Transport layer protocols like TCP and UDP are also supported. The most used protocol

are the Message Queuing Telemetry Transport (MQTT) protocol, the Advanced Message Queuing Protocol (AMQP), and the Data Distribution Service (DDS) [10].

3.1. COAP

CoAP (constrained application protocol) refers to the confined network protocol, a resource-limited application protocol that can be used on highly resource-restricted devices. It is a substitute for hypertext transfer protocol (HTTP), so it utilizes a petition and response model to facilitate providing services to IoT devices. CoAP is a well-known application protocol, particularly for the Internet of Things [11]. The following are the critical characteristics:

A. The CoAP protocol is combined with the User Datagram protocol, UDP.

B. It contains four fixes that ensure trustworthy packet forwarding.

C. It can send four messages: substantiated, non-confirmable, response, and reset.

3.2. MQTT

IBM first introduced Message Queue Telemetry Transport (MQTT) in 1999, and OASIS standardized it in 2013. Its purpose is to facilitate in-built connections between software components, such as applications and middleware, and infrastructure elements, such as networks and communications. Figure (3) depicts the publish/subscribe architecture used by the system; it consists of three primary parts: a creator, a consumer, and a trader are all involved. Publishers are equivalent to lightweight sensors that connect to a broker, transmit data, and then sleep on the Internet of Things. Applications that are interested in a specific topic or sensory data can sign up for updates from the brokers who collect and disseminate them. The brokers categories sensory data and distribute it to subscribers have demonstrated an interest in obtaining it [18].

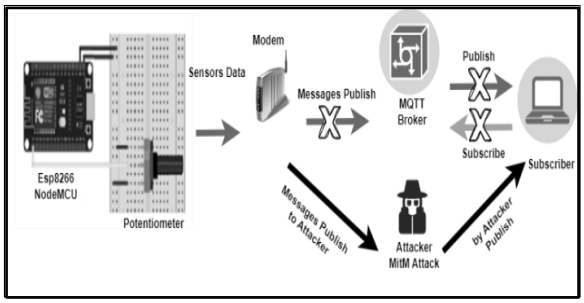

Figure.3 Man in the Middle Attack Scenario [18]

3.3. SMQTT

Secure MQTT (SMQTT) is an MQTT add-on utilizing minor authentication attributes to secure data. Broadcast encryption, which is commonly employed in Internet of Things (IoT) applications, offers a significant advantage., The effect on host List can be observed in figure (4) [12].

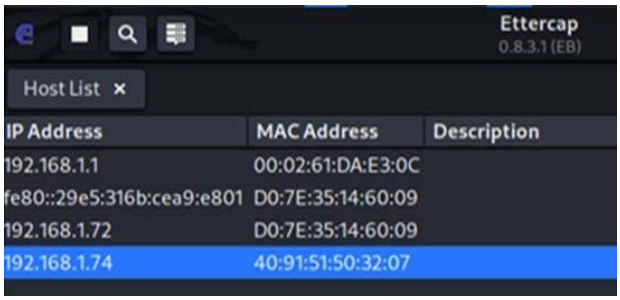

Figure.(4)IoT device identification by MAC address [31].

3.4 .AMQP

An Enhanced Queuing Protocol for Sending Messages It's perfect for financial transactions because it uses TCP protocol, transmission control layer security (TLS/SSL), and a confirmation architecture to communicate messages between devices [13].

3.5 .XMPP

Extended Messaging and Presence Protocol (XMPP) is used by real-time applications like instant messaging, phone calls, and video calls.

Extensible Markup Language is the data format (XML). Because XMPP is based on carelessness and forgetfulness, it does not provide high reliability. Although XMPP is a highly expandable protocol with many external plugins and capabilities, performance trade-offs are inevitable. So XMPP is out for this research due to the use case demanding high dependability, high throughput, and low latency [14].

3.6 . DDS

DDS data distribution service is a technology protocol for information publication communication. DDS's discovery service and 21-type QoS criteria secured a district corporation's data. However, DDS's features necessitate pre-work that reduces available resources, making it difficult to use in a resource-constrained setting [15].

4. Session Layer Protocols

Multiple standardization bodies have proposed protocols for the session layer of the Internet of Things, which is responsible for exchanging messages between devices. The Internet Protocol (TCP) and the User Datagram Protocol (UDP) are used by most IP applications, including IoT. However, some message distribution functions are standard among many IoT applications; these functions must be implemented using traditional interoperable methods by different apps. These are the so-called "Session Layer" [17].

5 . Security Aspects of IoT Protocol

The IoT domain's security and privacy concerns represent a wide range of threats to the entire system. As a result, the creation of a safe protocol for the Internet of Things is critical. It is not only about making things easier for people but also about lowering costs and increasing efficiency. The security of IoT protocols, as well as Internet of Things devices, which reflect the present growth of cellular connection, must be thoroughly examined. The technologies that will support 6G, the network's successor, are already attracting a lot of interest, despite the fact that the deployment of 5G cellular systems will take well into the next decade The Internet of Everything (IoE), which would require ubiquitous, stable, low-latency connectivity for up to a million devices per km² (terrestrial and aerial)

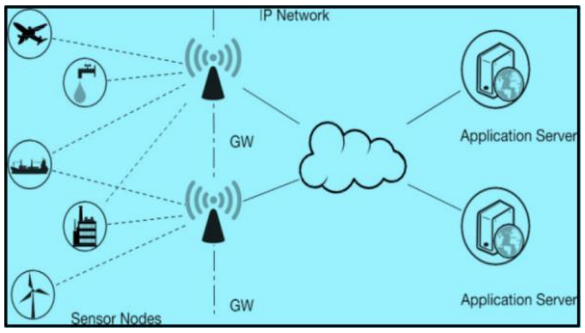

Figure. 5 IoT network architecture [19]

It is easy to send and receive text messages due to their lightweight and not taking up a large portion of the bandwidth from the spectrum used for communication , as shown in figure (4) [19].

6 . Actuators

Find out how transducers are being used in sensor networks in various contexts (IoT). An actuator is a gadget that can change things by converting electrical energy into usable energy for other gadgets. Components like heaters and air conditioners, speakers, lights, screens, and motors are all part of the package. Actuators that create motion can be split into three groups based on their way of operation: electrical actuators, hydraulic actuators, and pneumatic actuators, among others. Hydraulic actuators enable fluid-powered movement of mechanical components. Pneumatic actuators function under the pressure of compressed air, while Electric actuators operate under the force of electricity. That can be demonstrated using the illustration of a home control system, which consists of several Internet of Things. The actuators are in charge of locking and unlocking doors, turning on and off lighting, and other domestic appliances that warn users of potential dangers and regulate a home's temperature (via a thermostat). The digital thumb is one of the most innovative services on the Internet of Things. It can be used to turn on and off switches or do anything else that only needs a small amount of movement [32].

7 .Low-Power MAC-Layer Broadcast Frame

Tool Interaction Machine to Machine (M) is a technology for wireless network connectivity, with one of its most common applications being the Technology of the Future. M2M is becoming

increasingly popular and being utilized in various fields. In most situations, they are supplied by a cell that must be replaced with a power source regularly. This is a time-consuming operation in the majority of circumstances that may be causing the gadget to stop working. As a result, optimizing the energy usage of both the M2M equipment is a prudent move that will improve reliability while also saving money. One method for accomplishing this is incorporating a low-power communication network within the equipment. According to linked research findings, idleness and collisions are the two most significant contributors to energy consumption.
MAC protocol architecture that is power, as well as other ways that would aid in energy keeping, are considered. Moreover, a dual-emission Media Access Control (MAC) A protocol for machine-to-machine interactions is being developed. Grouping is the strategy employed in constructing the data transmission since it decreases the quantity of electricity consumed by the nodes while still engaging in the process correctly [20].

8. Confidentiality OF Cloud computing

As repeatedly indicated, the Internet of Things (IoT) is susceptible to numerous assaults that can potentially expose all crucial data and thus lead to bringing down the entire network infrastructure. Hence, coordinated strikes on different security systems wholly or partially compromised customers' information and IoT capabilities [20].

8.1 Block- Cyclic

It is one to consider as protection of confidentiality and trust-building technology. Therefore, using a set of time-stamped entries in a duplicated log file (also known as a ledger). Hence, the hash key is used to link each access to the one before it, and the bottom of the structure is saved in the blockchain; therefore, activities related to a specific connection can be validated at any time to guarantee they have not been tampered with. Architecturally, blockchains come in two varieties: allowed to access crypto connect, like virtual communication, would not enable users to follow a set of rules to join or leave the network. Because of the inherent secrecy and reliability provided by blockchains, IoT data may be kept secure on them. In addition to a larger surface area, code uses 256-bit passwords instead of storing data to secure the information A unique signature can be used to verify the authenticity of cloud-stored data during extraction to ensure the required confidentiality. Because of this, impersonating threats on code was prevented because devices could identify and affirm each other, avoiding rogue sites to users from being added. Blockchain naturally employs general populace secret keys in messaging to ensure that no entities have network access. As a result, this code serves as a foundation for data protection [21].

8.2 .Programming in the Cloud

Cloud technology serves as a bridge between premises processing and the gateway. Its primary The function is to process IoT data before transmitting it to the Internet so quick judgments can be made. There are two forms of a cloud environment. Therefore, cloud collection and storage are not required in the fog microarchitecture, which is needed for both data centers. At the same time, edge devices are part of taking decisions and making superficial judgments, while a central server is used. For essential choices. It is required that all demands pass through this critical stage, which will, in essence, overcome many attacks, such as player threats and data transportation threats. To avoid making bad judgments, it offers options to expose questionable data or demands prevent denial-of-service attacks (DOS) [22], as shown in Table 1.

9 Conclusion

The proper communication protocols must be studied in order to connect the enormous number of Internet of Things (IoT) devices with the central servers. To ensure the reliability, ease, and security of communications devices for smart cities, we made a choice of the protocol Message Queuing Telemetry Transport (MQTT). Represents the best type of other types of communication protocols? It is characterized as lightweight in terms of storage, flexible in handling, and secure in terms of penetration and espionage on the communications networks; therefore, it is an important and necessary goal that we set for this research paper. As a result, we advise that the MQTT protocol be encrypted in order to connect IoT devices with central servers. Therefore, this work will make the communication layers safe and highly reliable when used in modern communication devices in the future.

References:

[1] Khan, Wazir Zada, et al. *"Industrial internet of things: Recent advances, enabling technologies and openchallenges."*Computers&ElectricalEngineering 81(2020):106522

[2] HaddadPajouh, H., Dehghantanha, A., Parizi, R. M., Aledhari, M., & Karimipour, H. (2021). *A survey on internet of things security*: Requirements, challenges, and solutions. Internet of Things, 14, 100129.

[3] Rajesh, P., Shajin, F. H., & Kannayeram, G. (2022). *A novel intelligent technique for energy management in smart home using internet of things.* Applied Soft Computing, 128, 109442.

[4] Mashaleh, A. S., Ibrahim, N. F. B., Alauthman, M., Almseidin, M., & Gawanmeh, A. (2024). *IoT Smart Devices Risk Assessment Model Using Fuzzy Logic and PSO*. Computers, Materials & Continua, 78(2).

[5] Silva, T., Casal, J., & Chaves, R. (2023, October). *Lightweight network-based IoT device authentication in Cloud services*. In 2023 IEEE 31st International Conference on Network Protocols (ICNP) (pp. 1-6). IEEE.

[6] Li, D. F., Kasemsap, K., Yager, R. R., Crockett, K., Liu, P., Jensen, R., ... & Li, Y. (2020). *International Journal of Fuzzy System Applications. International Journal*, 9(1).

[6] Sankar, S., and P. Srinivasan. "*Internet of Things based digital lock system." Journal of Computational and Theoretical Nanoscience15*.9-10(2018):2758-2763.

[7] Rocha, Clarissa, Clariana Fernandes Narcizo, and Enrico Gianotti. *"Internet of management artifacts: Internet of Things architecture for business model renewal."* Emerging Issues And Trends In Innovation And Technology Management. 2022. 297- 316.

[8] Kumar, K., Kumar, A., Kumar, N., Mohammed, M. A., Al-Waisy, A. S., Jaber, M. M., ... & Al-Andoli, M. N. (2022). Dimensions of internet of things: *Technological taxonomy architecture applications and open challenges—a systematic review.* Wireless Communications and Mobile Computing, 2022.

[9] Gupta, P. (2021, June). *A survey of application layer protocols for internet of things*. In 2021 International Conference on Communication information and Computing Technology (ICCICT) (pp. 1-6). IEEE.

[10] Makarem, N., Diab, W. B., Mougharbel, I., & Malouch, N. (2022). On the design of efficient congestion control for the Constrained Application Protocol in IoT. Computer Networks, 207, 108824.

[11] Ali, J., & Zafar, M. H. (2023). *Improved End-to-end service assurance and mathematical modelling of message queuing telemetry transport protocol based massively deployed fully functional devices in smart cities. Alexandria Engineering Journal*, 72, 657-672.

[12] Anna, Dheeraj Manirathnam, M. N. Vijayalakshmi, and Solomon Raju Kota. "*Enabling lightweight device authentication in message queuing telemetry transport protocol*." IEEE Internet of Things Journal 11.9 (2024): 15792-15807.

[13] Anna, D. M., Vijayalakshmi, M. N., & Kota, S. R. (2024). *Enabling lightweight device authentication in message queuing telemetry transport protocol. IEEE Internet of Things Journal*, 11(9), 15792-15807.

[13] Wang, Z. (2023). *Mobility digital twin with connected vehicles and cloud computing.* Authored Preprints.

[14] Iskandarani, M. Z. (2024, November). Communication *Analysis of Wireless Sensor Networks with Mobility Function*. In 2024 4th International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME) (pp. 1-6). IEEE.

[15] Aheleroff, S., Xu, X., Lu, Y., Aristizabal, M., Velásquez, J. P., Joa, B., & Valencia, Y. (2020). *IoT-enabled smart appliances under industry 4.0: A case study*. Advanced engineering informatics.

[16] NURUS SALAM, M. O. H. A. M. M. A. D. *Modelling of a Communication Protocol for IoT based applications*. Diss. DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING,2021.

[17] Ati, Mustafa K. "*Managing smart cities by designing a communications system using LoRa*

technology." The Nexus of Sustainability and Energy Technology Journal 1.1 (2025): 1-6.

[18] Aski, V. J., Dhaka, V. S., Parashar, A., & Rida, I. (2023). Internet of Things in healthcare: *A survey on protocol standards,enabling technologies, WBAN architectures and open issues. Physical Communication*, 60, 102103.

[19] Jha, Sujeet Kumar, and Abhishrii Puri. "*Energy-Efficient MAC Layer Protocol for Communication."* network8.07 (2021).

[20] Mohammad, N., Khatoon, R., Nilima, S. I., Akter, J., Kamruzzaman, M., & Sozib, H. M. (2024). *Ensuring Security and Privacy in the Internet of Things: Challenges and Solutions. Journal of Computer and Communications,* 12(8), 257-277.

[21] Hassan, M., Hussein, A., Nassr, A. A., Karoumi, R., Sayed,U. M., & Abdelraheem, M. (2024). *Optimizing structural health monitoring systems through integrated fog and cloud computing within IoT framework*. IEEE Access.

[22] Burhan, M., Alam, H., Arsalan, A., Rehman, R. A.,Anwar, M., Faheem, M., & Ashraf, M. W. (2023). *A comprehensive survey on the cooperation of fog computing paradigm-based iot applications: layered architecture, real-time security issues, and solutions*. IEEE Access.

[23] Bajaj, K., Sharma, B., & Singh, R. (2021, September). *Edge, fog and cloud-based smart communications for IoT network based services & applications*. In 2021 International Conference on Artificial Intelligence and Machine Vision (AIMV) (pp. 1-5). IEEE.

[24] Sobin, C. C. "*A survey on architecture, protocols, and challenges in IoT*." Wireless Personal Communications 112.3 (2020): 1383-1429.

[25] Tariq, M. A., Khan, M., Raza Khan, M. T., & Kim, D. (2020). *Enhancements and challenges in coap—a survey*. Sensors, 20(21), 6391.

[26] Furstenau, L. B., Rodrigues, Y. P. R., Sott, M. K., Leivas,P., Dohan, M. S., López-Robles, J. R., ... & Choo, K. K. R. (2023). *Internet of things: Conceptual network structure, main challenges and future directions. Digital Communications and Networks*, 9(3), 677-687.

[27] Goar, V. (2022). 6LoWPAN in *Wireless Sensor Network with IoT in 5G Technology for Network Secure Routing and Energy Efficiency. International Journal on Future Revolution in Computer Science &Amp*, 15-25.

[28] Yar, H., Imran, A. S., Khan, Z. A., Sajjad, M., & Kastrati,Z. (2021). *Towards smart home automation using IoT-enabled edge-computing paradigm. Sensors*, 21(14), 4932.

[29] Weqar, M., Mehfuz, S., Gupta, D., & Urooj, S. (2024). *Adaptive Switching Based Data-Communication Model for Internet of Healthcare Things Networks*. IEEE Access.

[30] Kamruzzaman, M. M. (2022). *Key technologies, applications and trends of internet of things for energy-efficient 6G wireless communication in smart cities. Energies*, 15(15), 5608.

[31] Şimşek, Mustafa Muhammed, and Emrah Atılgan. "*Attacks on availability of iot middleware protocols: A case study on mqtt*." Eskişehir Türk Dünyası Uygulama ve Araştırma Merkezi Bilişim Dergisi 4.2 (2023): 16-27.

[32] Azad, T., Newton, M. H., Trevathan, J., & Sattar, A. (2025). IoT edge network interoperability. Computer Communications, 236, 108125.

TABLE 1

A COMPARISON BETWEEN IOT COMMON PROTOCOLS

Comparison Key	Stands for	Description	Layer	Goal
COAP	Constrain need Application Protocol	Engrained methods involve UDP to transmit data over limited circuits and this depicts how it works IoT [25].	Application Layer	To conserve energy, it is typically employed to transmit weak signals. .
MQTT	Message Queuing Telemetry Transport Protocol	specifies the customer's paradigm for transmitting signals to the Middleware and getting response from users [26].	Application Layer	Comfortable accessibility and little protocol weight. Numerous Internet of Things use cases are supported. It also supports transmission layer security via Transport Layer Security (TLS/SSL) [30].
IPV6	Internet protocol V6	Due to restrictions on foreign IPs, IPV4 can meet demand but is unable to serve those sites and the previously associated one [27].	Transport Layer	In addition to its basic work in maintaining communication between devices, also it is being used to get around IPv4 restrictions.
6LOW PAN	IPV6 over Low power wireless personal area networks	It is built on top of IEEE 802.15.4 and is used to transmit data via low-latency cognitive radio networks, which helps save money and time on monitoring equipment [28].	Convergence Layer	It also is used to transfer data through IPv6 while using very little energy.
ZigBee	Zonal Interco Communi-cation Global- standard	Its working principle depends on The Wi-Fi module adheres to the stringent energy and management standards of the Internet of Things [29].	MAC Layer	is frequently employed to provide a cheap data connection between mobile devices but has limited range.

Contributor Roles Taxonomy (CRediT)

Conceptualization	Comparing communication protocols and choosing the best protocol with all features and developing it.
Data curation	Advantages and disadvantages of communication protocols based on previous and recent experiences.
Formal analysis	The applications of communication protocols on drones and their connection to satellites and to an advanced communication protocol were studied.
Investigation	Each communication protocol has advantages that can be developed, and we have developed a modern communication protocol that keeps pace with the development of modern devices.
Methodology	A research methodology was adopted that relies on the results of previous research and develops those results according to the new data.
Project administration	The speed and security of the modern communication protocol was the main focus of my research.
Resources	Previous studies and research.
Software	Add programming encryption of transmitted and received data.
Supervision	Can application on modern network communication in future.
Validation	Take all previous results, so development the communication protocol.
Visualization	Encryption and decryption the communication protocol.
Writing – original draft	Depending on all previous data , after that developed it.
Writing - review & editing	Explained in table. 1 , the end of this research.
Funding acquisition	No funding acquisition.