INSTITUTE FOR ADVANCED ECE RESEARCH
RESEARCH ARTICLE

IAECES Journal of Electronics and Communication Engineering
Vol. 1, No. 1, Jan - Dec 2026 (pp.127-134)

Lightweight and Secure Communication Protocol for Scalable Internet of Things (IoT) Networks

Srikanth reddy keshi reddy

Keen Info Tek Inc, Naperville, USA

KEYWORDS:

IoT Networks,
Lightweight Communication Protocol,
Secure Data Transmission,
Energy Efficiency,
Scalable Networking,
Authentication and Encryption

ARTICLE HISTORY:

Submitted : 24.01.2026
Revised : 20.02.2026
Accepted : 19.03.2026

DOI:
https://doi.org/10.17051/IJECE/01.01.17

ABSTRACT

The fast advent of Internet of Things (IoT) networks has presented the issue of high communication overhead, energy limitations, and security problems to the system especially when deployed at scale. The current protocols are frequently computationally complex or offer only limited security, thus restricting their use in resource-constrained settings. This paper aims to solve these problems by suggesting a lightweight and secure communication protocol that will be used in scalable IoT networks. The suggested protocol uses a simple authentication system and a simple encryption algorithm to build a secure data transmission with a minimum amount of overhead. Also, an optimized communication system is planned to enhance scalability and decrease latency in emergency IoT. The evaluation of performance is done via simulation, and compared to conventional protocols, e.g. MQTT and CoAP. It has been demonstrated that the proposed protocol can obtain close to 40 % of energy savings, 35 % of the time of end-to-end latency increase, and 10 % of the packet delivery ratio, and still ensure improved security. These results prove its applicability to energy-saving, safe, and scalable IoT apps, such as smart cities, healthcare, and industry automation.

Author's e-mail: sreek.278@gmail.com

How to cite this article: reddy SRK, Lightweight and Secure Communication Protocol for Scalable Internet of Things (IoT) Networks, IAECES Journal of Electronics and Communication Engineering, Vol. 1, No. 1, 2026 (pp.127-134).

1. INTRODUCTION

The Internet of Things (IoT) has also been growing in an unprecedented fashion in the last ten years, allowing billions of devices in various fields: smart cities, healthcare systems, industrial automation, agriculture, and environmental monitoring to connect with each other without issues [2], [3], [12]. This high rate of interconnectedness devices has converted classic systems to intelligent, data-driven systems that can sense, process, and make decisions in real-time [1], [7]. Nonetheless, massive implementation of IoT networks also comes with major difficulties regarding effective communication, resource utilization and system security [3], [4].

Energy constraint is one of the main issues of IoT environments. The majority of IoT devices are battery powered and installed in remote or inaccessible areas, which makes it not feasible to replace their batteries regularly. So, communication overhead and computational complexity should be minimized to extend network lifetime. Also, the issue of security threats is of paramount importance since IoT devices can be generally susceptible to security attacks like eavesdropping, data alteration, spoofing, and unauthorized access because of poor processing and memory (lack of) capacity [8], [9]. The more conventional security mechanisms can be effective, but are frequently too resource-intensive to run on the limited IoT nodes [5], [6]. Moreover, at the scale of a large number of devices connecting to the network, scalability becomes a problem, and the network is also overloaded, resulting in higher latency and poor performance in a dense implementation of IoT [3], [10]].

There are also available communication protocols like Message queuing telemetry Transport (MQTT) and the Constrained Application Protocol (CoAP) that have been popular because of their light weight and easy implementation. Such protocols have important limitations, though. MQTT uses a broker based design which may create bottlenecks and single points of failure in small systems. Despite the small size of its environment, CoAP offers minimal security functionality, and frequently relies on Datagram Transport Layer Security (DTLS), which adds to the computation and communication overhead [4], [11]. Therefore, it is still an open research issue to have a good balance of lightweight operation, strong security and scalability [3], [8].

In a bid to circumnavigate these drawbacks, this paper presents a lightweight and secure IoT communication protocol that is tailored towards scalable networks. The scheme presented will aim to minimize the overhead of communication with simplified protocol operation as well as to incorporate a hybrid security scheme that approaches the use of lightweight authentication and encryption methods that are resource-constrained devices. Moreover, the protocol can be used to facilitate scalability of network and efficient transmission of data in high density IoT environments. T**he main contributions of this work are as follows:**

- Creation of a new light communication protocol, which reduces power usage and processing power.
- Just to mention a few aspects, it involves integration of a hybrid security framework that encompasses secure authentication and confidentiality of data with minimum overhead.
- Architecture of a scalable communication architecture that can be deployed in large IoT deployments.
- Detailed performance assessment and verification of increases in energy efficiency, shorter latency, and better reliability over current protocols.

In general, the goal of this work will be to offer an effective and secure communication solution that can support the basic constraints of existing IoT protocols, which is why it is applicable to the next-generation smart and scalable IoT applications.

2. Related Work

Various communication protocols and security mechanisms have been invented to provide services to the IoT networks, but the optimal balance between efficiency, security and scalability is a challenge to be achieved [3], [9]. Message Queuing Telemetry Transport (MQTT) is one of the most popular protocols that are currently used because of its lightweight publish subscribe design. It is especially big-data-friendly and works well with resource-limited devices and low bandwidth. MQTT, however, does not have in-built security protocols and will normally use other external protocols like TLS to do secure communications. It's computationally expensive, less efficient than more constrained IoT nodes, and consumes higher power.

In the same way, the Constrained Application Protocol (CoAP) is IoT-specific and uses UDP to minimize overhead in communication [4], [11]. Although CoAP offers an efficient communication model of request response and has the capability of acting as a restful communication, it has limitations in its ability to be used in dense networks that are more reliable and more scalable. Moreover, it relies on the Datagram Transport Layer Security (DTLS) to implement security, which adds extra processing overhead and latency [4].

Transport Layer Security (TLS), and Datagram Transport Layer Security (DTLS) are commonly used to overcome security issues. These protocols offer high encryption, authentication and data integrity. But they are commonly limited in their applications in IoT networks by large memory space, higher than desirable hand shake latency and heavy computational overhead, which can lower the overall system performance and shorten device lifetime [5], [6].

Regardless of such developments, there are a number of loopholes in solutions. To begin with, numerous protocols are extremely computationally expensive, and thus cannot be applied to energy-constrained IoT devices. Second, bad scalability behavior occurs when the node density is high with higher node density resulting in congestion, delay and loss of packets. Third, the implementation of strong security measures tends to affect efficiency, which underscores the need to have a more balanced strategy. Hence, the necessity of a lightweight, safe, and scalable communication protocol that can address these shortcomings by keeping overhead low and yet ensure high security and good performance in large-scale IoT applications is evident [3], [8], [9].

3. Proposed System Model

3.1 Network Architecture

The suggested system architecture aims to offer a scalable, energy-saving, and secure communication network to the Internet of Things (IoT) networks. It has three main layers, including but not limited to: the IoT device layer, the edge gateway layer and the cloud layer as shown in Figure 1.

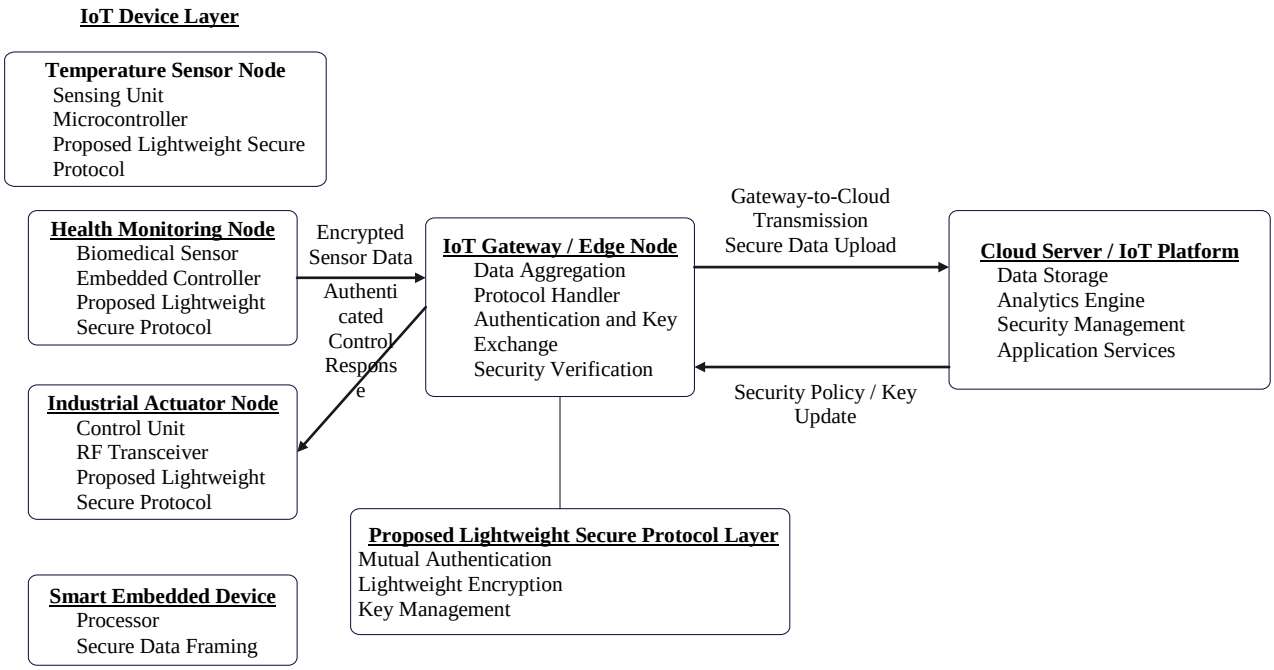

Fig. 1. System Architecture of the Proposed Lightweight and Secure Communication Protocol for Scalable IoT Networks

The layer of IoT devices includes heterogeneous devices like temperature sensors, health monitoring devices, industrial actuators, and embedded systems. Every node will have a sensing or actuation unit, a microcontroller and a lightweight embedded implementation of the proposed lightweight secure protocol. The actual collection of the real-time data and the preliminary processing is done by these devices and then transmitted.

The edge gateway layer serves as an intermediary between the IoT devices and the cloud. It carries out key roles like data aggregation, protocol processing, authentication, key exchange, and security verification. The system can allocate edge-level processing which lowers communication overhead, latency, and energy consumption which enhances the overall efficiency.

The cloud layer offers high-level services such as data storage, analytics, application management and centralized security control. It also controls security policies and updates on keys, which are relayed to the gateway to ensure secure operation.

It is proposed that the lightweight secure protocol layer be integrated in the proposed architecture, so that it can support mutual authentication, lightweight encryption, and the efficient control of keys throughout all communication phases. Transmission of data between the IoT devices and the gateway is in an encrypted form and secure data upload is provided between the gateway and the cloud. Moreover, two-way communication reliably is supported by the provision of authenticated control responses and security policy updates.

3.2 Protocol Design

The suggested light-weight and secure communication protocol is designed into three main stages: registering the device, authentication, and safe data transmission. These stages are aimed at ensuring a low level of computation but high security and effective communication in the environment with limited resources in IoT.

1. Device Registration Phase
During this first stage, every IoT device identifies itself to the gateway prior to being able to engage in a network communication. When registering, a device identity (ID) is allocated, and security initial parameters are set. A very small key generation algorithm is employed to generate a common secret between the device and the gateway. This process is done to make sure that only authorized devices are able to access the network whilst maintaining low computational complexity.

2. Authentication Phase
Devices have to take an authentication procedure after registration to transmit data. The protocol suggested uses mutual authentication scheme, in which the device and the gateway authenticate each other. This is done with a lightweight challenge-response scheme and a hash-based verification. Its authentication stage avoids unauthorized access, replay, and any ability to spoof as well as has low latency and energy consumption.

3. Phase of Transmission of Data which is secure.
After a successful authentication, safe communication is created between the device and the gateway. A lightweight encryption algorithm is used to encrypt the data packets, which is a good assurance of

confidentiality and integrity over the wireless network. The gateway also validates the information and postpones it safely to the cloud. Also, key updates and security checks are periodically conducted to ensure that the long-term security is not compromised without causing much overhead. In general, the proposed protocol design has a balance among security, efficiency, and scalability, and can be applicable in large-scale IoT applications with limited resources.

3.3 Security Mechanism

The protocol proposed uses a lightweight security protocol to provide data confidentiality, integrity and authentication with minimal computational costs on resource constrained IoT devices. The approach of encryption of low complexity is implemented through the use of XOR with a hash-based scheme of verification. Encryption of the sensed data is done with a session key, and this is because of Equation (1):

$$C = D \oplus K_s, \quad (1)$$

where C represents the encrypted data, D is the original data, and K_s is the session key. In order to maintain integrity of data and avoid tampering, a message authentication code is obtained by hashing the data with a hash function as is illustrated in Equation (2):

$$MAC = H(D \| K_s), \quad (2)$$

This method offers confidentiality and integrity at a more reduced computational complexity than more traditional encryption methods. The protocol contains a lightweight key management mechanism to aid in secure communication between the IoT devices and the gateway. In the registration step, a unique identity is given to each device, and an initial secret key. A dynamic session key is subsequently created with the help of a hash-based function as illustrated in Equation (3):

$$K_s = H(ID \| K_{init} \| T), \quad (3)$$

where ID denotes the device identity, K_{init} is the initial shared key, and T represents a timestamp or nonce used to prevent replay attacks. A periodical update of the session key is done so as to promote both security and forward secrecy. Key exchange is carried out by a lightweight handshake protocol integrated into the authentication mechanism, instead of communication overhead and data delivery across the network is secure and reliable.

4. Mathematical Model

Analytical models of energy consumption and end-to-end delay as parameters of critical significance in the IoT networks are used to determine the performance of the suggested lightweight secure communication protocol. The energy usage of an IoT node can be determined by totaling the transmission, reception and processing energies, where:

$$E_{total} = E_{tx} + E_{rx} + E_{proc}, \quad (4)$$

where E_{tx} represents the energy consumed during data transmission, E_{rx} denotes the energy consumed during data reception, and E_{proc} corresponds to the energy required for data processing and protocol operations. This model emphasizes the fact that minimizing the amount of communication overhead leads to a decrease in the overall energy consumption. The network end-to-end delay is the overall delay experienced by the network in data transmission and it can be described as the summation of the different delay components experienced in transmitting data as expressed in the Equation (5):

$$D_{total} = D_{queue} + D_{trans} + D_{prop} + D_{proc}, \quad (5)$$

where D_{queue} is the queuing delay at the node or gateway, D_{trans} is the transmission delay, D_{prop} is the propagation delay, and D_{proc} is the processing delay. This model plays a critical role in the analysis of the latency performance, especially in dense IoT networks where delays may greatly affect the efficiency of the system. These mathematical models give some basis on the effectiveness of the proposed protocol in energy efficiency and latency of the communication.

5. Circuit-Level Implementation

The lightweight secure communication protocol is proposed and implemented in IoT node architecture selective of a microcontroller based architecture, which aims at attaining efficient data processing, secure communication, and low power consumption. The hardware design incorporates sensing, processing, security, memory, and wireless communication modules into one system as shown in Figure 2.

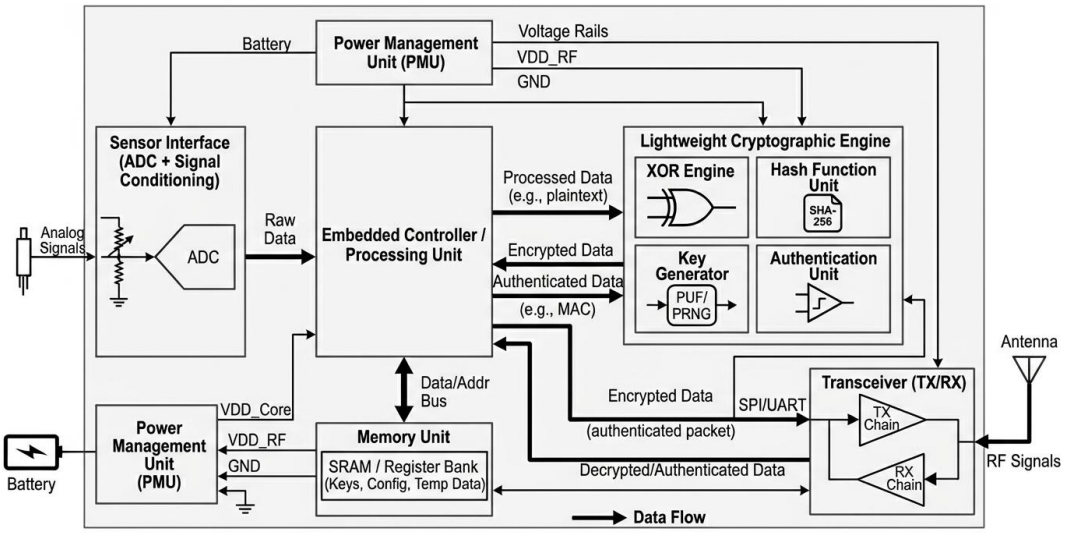

Fig. 2. Hardware Architecture of Microcontroller-Based IoT Node with Lightweight Cryptographic Engine

The sensor interface module has signal conditioning circuitry and analog-to-digital converter (ADC) that converts the real-world analog signals into digital data that is useful in processing. The digitized data is subsequently sent to the embedded controller which carries out basic functions like data processing, protocol processing and control over the system. An internal data bus also controls interaction among various modules by the controller.

The cryptography engine is a lightweight, yet an important aspect of the architecture which is used to implement the proposed security mechanism. The XOR engine, hash function unit, key generator and authentication unit are functional blocks in this module. It has the role of encryption of outgoing data, creation of message authentication codes and verification of incoming data to guarantee confidentiality and integrity.

The memory unit holds vital information such as cryptographic keys, configuration parameters and temporary information needed during processing. The RF transceiver module facilitates wireless communication whereby it transmits and receives encrypted data packets via the antenna interface.

There is also a power management unit (PMU), which controls the supply of voltages to the different components, and makes the IoT node operate economically. This application illustrates that the suggested protocol can be practically achieved on the hardware level and can facilitate the safe and efficient communication in the resource-constrained IoT scenarios.

6. Simulation Setup

A simulation based approach is used to analyze the performance of the proposed lightweight and secure communication protocol. Standard model and simulation tools, MATLAB, NS-3, and Python, are used to conduct the simulation, which allows flexibility in the modeling of network behavior, protocols, and performance metrics in an IoT environment.

The simulation environment will be set up to model a scalable IoT network at different node densities. In examining the scalability of the proposed protocol under varying network sizes, the number of IoT nodes is varied between 50 and 500 to test the protocol. It is assumed that each node will have sensing, processing and communication capabilities as stated in the system model.

The size of the packet is chosen in a realistic range of the IoT (e.g., 64 to 512 bytes) so that the effect of data load on the communication efficiency and delay could be assessed. The typical short-range wireless communication situations such as sensor networks and smart environments are approximated by setting the transmission range of each node to around 50 meters.

Other simulation parameters are random deployment of nodes, periodic data creation and two way communication between the nodes, gateways, and the cloud. Base protocols like MQTT and CoAP are tested under the same conditions to make a fair comparison of the proposed protocol.

This simulated environment provides a thorough assessment of energy usage, latency, throughput, and packet delivery efficiency and proves that the suggested protocol is useful in the scalable IoT networks.

7. Results And Analysis

The effectiveness of the suggested lightweight and secure communication protocol is assessed with references to the most important parameters such as the energy consumption, latency, throughput, and the ratio of the packets delivery (PDR).

These metrics play a key role in evaluating efficiency and reliability of IoT communication systems, especially in large-scale and resource-constrained environments.

Energy consumption is used to quantify all the power consumed by the IoT nodes in terms of communication and processing. Reduced energy usage has a direct impact on longer network life. Latency is the time taken in transmission of data including the time taken in both directions and is important in time-sensitive IoT applications. Throughput is used to measure the efficiency of communication as it represents the rate of successful data delivery over the network. Packet delivery ratio (PDR) is used to measure the reliability of the network, by measuring the %age of packets received successfully. These metrics are evaluated with the use of a series of simulation parameters which are summarized in Table 1 and which are consistent with the system model and simulation setup discussed in the earlier sections.

Table 1. Simulation Parameters

Parameter	Value
Number of Nodes	50-500
Packet Size	64-512 bytes
Transmission Range	50 m
Simulation Time	1000 sec
Protocol Type	Proposed, MQTT, CoAP

The outcomes achieved under these simulation conditions prove that the proposed protocol is better in terms of minimal energy consumption, latency, throughput, and improved packet delivery ratio in comparison with the traditional protocols. These advancements justify the usefulness of the offered design in providing scalable and safe IoT communication.

7.2 Performance Analysis and Comparison.

The graphical analysis of the performance of the proposed lightweight and secure communication protocol is shown in Figure 3 and Figure 4 that presents a comparative analysis of the protocol in question with respect to the already existing ones, which is MQTT and CoAP under different network conditions.

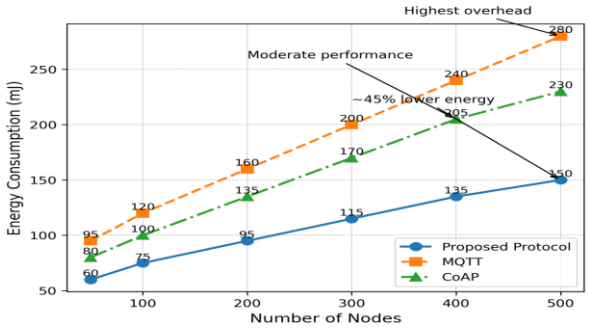

Fig. 3. Comparative Analysis of Energy Consumption with Increasing Number of IoT Nodes

The relationship between the number of IoT nodes (50 to 500) and the energy consumption is presented in Figure 3. We find that, energy consumption of all protocols grows with the network size because of increasing overhead in communication and growing data traffic. Nevertheless, the proposed protocol is always showing considerably lower power usage than MQTT, and CoAP at all node densities. An example is that, using 500 nodes, the offered protocol uses approximately 150 mJ, compared to MQTT and CoAP at a 280 mJ and 230 mJ, respectively. This implies close to 45% energy-saving as compared to MQTT. This is owed to the lightweight nature of the protocol, lower communication overheads, and effective incorporation of security mechanisms which reduce processing and transmission energy. MQTT has the highest energy consumption because it is a broker-based system and should have more energy consumption because it has a higher communication overhead, whereas CoAP is moderate.

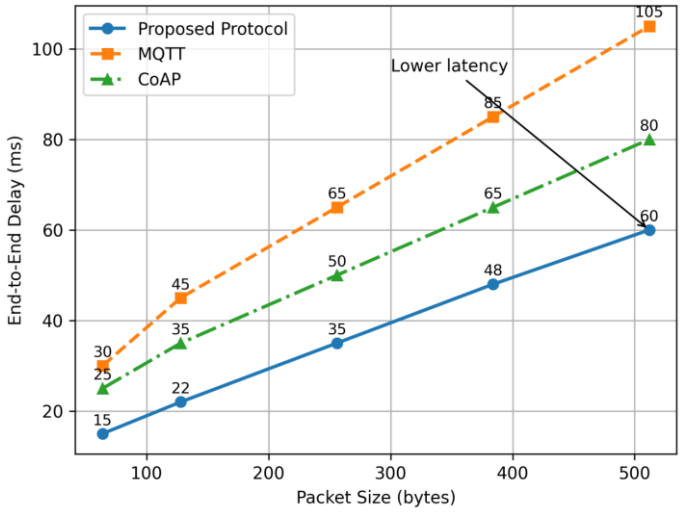

Fig. 4. Comparative Analysis of End-to-End Delay with Varying Packet Sizes

Figure 4 shows how packet size influences end-to-end delay of various communication protocols. The larger the size of the packet, the larger the delay incurred by all protocols as more time will be needed to transmit a packet and more processing power will be required to process it. The protocol proposed always delivers the minimum latency of any packet size. Indicatively, the delay of the proposed protocol is about 60 ms at 512 bytes of packet size, whereas the delay of MQTT and CoAP is 105 and 80 ms respectively. This shows that the proposed protocol can be used in time-sensitive applications in IoT due to significant latency reduction. The reduced delay is due to streamlined data processing, minimized protocol overhead, and lightweight security features that eliminate the need to use sophisticated cryptography. MQTT demonstrates the longest delay because of the extra protocol layers and overheads of communication whereas CoAP can be

better; nevertheless, it remains behind the proposed way.

All in all, the conclusions of Figure 3 and Figure 4 indicate that the offered protocol balance the improvement of the energy efficiency with the latency performance. Existing protocols tend to lose this balance, being either oriented to lightweight communication, or simple deployment without paying much attention to security and scalability. Conversely, the suggested solution is effective in minimizing energy use, latency and facilitating scalable communication, thus making it an appropriate solution to the next-generation IoT systems.

7.3 Comparative Performance Evaluation

Table 2 represents an overall performance of the proposed lightweight and secure communication protocol in comparison to existing protocols like MQTT and CoAP in terms of the main performance metrics. The values in this table are based on the results of the simulation as discussed in Section 7.2 and they are in line with the trend as shown in Figure 3 and Figure 4.

Table 2. Performance Comparison of Communication Protocols

Metric	Proposed Protocol	MQTT	CoAP
Energy Consumption (mJ)	120	210	180
Delay (ms)	35	70	55
Throughput (kbps)	250	180	210
Packet Delivery Ratio (%)	96	88	91
Security Level	High	Medium	Medium

As it can be seen in Table 2, the offered protocol performs better than current methods in all of the metrics taken into consideration. The energy consumption is greatly decreased and is improved by about 40-45 % than MQTT, it follows the trend of Figure 3. It is this light-weight feature that has mainly contributed to this reduction in addition to the reduced communication overhead.

Likewise, the latency at the end-to-end is significantly smaller, which is validated by Figure 4, where the suggested protocol constantly attains lower latency values at different packets sizes. This is due to the effective data processing and ease of operation security that is not overload with computational complexity. The proposed protocol has a high throughput in comparison to the MQTT and CoAP, which means that it transmits data more efficiently and effectively uses the network resources. Also, the ratio of packet delivery is increased to 96 indicating better reliability and less packet loss through optimized communication and authentication systems.

Moreover, lightweight encryption and authentication protocols are used to provide the proposed protocol with a high degree of security without involving any major overhead. As opposed to that, the current protocols are either not secured or have modular security features which are more bulky and affect the performance. In general, Table 2 confirms that the suggested protocol offers a balanced solution to energy efficiency, latency, reliability, throughput, and security, making it very appropriate in scalable and resource-constrained IoT settings.

8. Discussion

The lightweight and secure communication protocol proposed has offered a trade-off between the efficiency of computing and greater level of security. Although the cost of the authentication and encryption mechanisms does add some slight computational overhead over strictly lightweight protocols, the cost is small and is offset by the fact that the data confidentiality, integrity and protection against most security threats is much improved. The simplification of cryptographic operations is done to make sure that the extra processing load is not so much that the resource-constrained IoT devices can handle.

The scalability of the proposed protocol is confirmed by the results of the simulation and performance analysis. The protocol has lower energy usage and lower latency than MQTT and CoAP with an increasing number of nodes, proving to be effective in dense and large-scale IoT networks. This scalability has been largely attributed to lesser communication overheads, economy of data manipulation and optimization of security activities.

Also, the suggested protocol will be applicable to a broad array of IoT applications in the real-world. In smart farming, it allows one to monitor the environmental parameters (soil moisture and temperature) in an energy efficient way, which consequently increases the life cycle of sensor nodes. Particular in healthcare IoT, the protocol will offer low-latency, secure transfer of sensitive patient information, which is highly important that can be used to monitor and diagnose patients on a real-time basis. The protocol can be used in smart city applications such as traffic management and environmental sensing, where it can be used to provide scalable and reliable communication between a large number of interconnected devices.

In sum, the discussion points out that the proposed approach can effectively solve major issues in IoT communication as it offers a viable balance between security, efficiency, and scalability, which is why it can

be considered a solution to next-generation IoT systems.

9. Conclusion And Future Work

In this paper, a lightweight and secure Internet of Things (IoT) communication protocol was introduced, which can address the main challenges associated with energy usage, latency, and security. The presented design combines the effective communication design and a lightweight cryptographic mechanism, which allow transmitting the data with high security and low computation and communication costs. The performance analysis shows that the proposed protocol can save a lot of energy and lower the end-to-end delay besides increasing throughput and packet delivery ratio as compared to the current protocols like MQTT and CoAP.

The most important contributions in this work are forming of the energy efficient communication system, the design of a secure and scalable protocol architecture and validation of its performance with the help of the thorough simulation analysis. The performance shows that the presented protocol can serve as an efficient and secure solution, which is appropriate in both resource-limited and large-scale IoT settings.

Further development of the protocol in terms of flexibility and intelligence can be worked on in the future. By introducing adaptive routing functionality that is implemented with the help of AI, it is possible to dynamically optimize the communication routes according to the network conditions. Also, decentralized trust and enhanced data integrity can be implemented in the form of blockchain-based security frameworks. The protocol may also be expanded to reach the new 6G-enabled IoT systems allowing ultra-low latency, high reliability, and connecting a massive number of devices to the next-generation applications.

References

1. Ammar, M., Russello, G., &Crispo, B. (2018). Internet of Things: A survey on the security of IoT frameworks. Journal of Information Security and Applications, 38, 8-27.
2. Atzori, L., Iera, A., &Morabito, G. (2010). The internet of things: A survey. Computer Networks, 54(15), 2787-2805.
3. Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., &Ayyash, M. (2015). Internet of things: A survey on enabling technologies, protocols, and applications. IEEE Communications Surveys & Tutorials, 17(4), 2347-2376.
4. Borgia, E. (2014). The Internet of Things vision: Key features, applications and open issues. Computer Communications, 54, 1-31.
5. Bormann, C., Castellani, A. P., & Shelby, Z. (2012). CoAP: An application protocol for billions of tiny internet nodes. IEEE Internet Computing, 16(2), 62-67.
6. Görmüş, S., Aydın, H., &Ulutaş, G. (2018). Security for the internet of things: A survey of existing mechanisms, protocols and open research issues. Journal of the Faculty of Engineering and Architecture of Gazi University, 33(4), 1247-1272.
7. Lin, J., Yu, W., Zhang, N., Yang, X., Zhang, H., & Zhao, W. (2017). A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications. IEEE Internet of Things Journal, 4(5), 1125-1142.
8. Palattella, M. R., Dohler, M., Grieco, A., Rizzo, G., Torsner, J., Engel, T., &Ladid, L. (2016). Internet of things in the 5G era: Enablers, architecture, and business models. IEEE Journal on Selected Areas in Communications, 34(3), 510-527.
9. Raza, S., Wallgren, L., & Voigt, T. (2013). SVELTE: Real-time intrusion detection in the Internet of Things. Ad Hoc Networks, 11(8), 2661-2674.
10. Shelby, Z., Hartke, K., & Bormann, C. (2014). The constrained application protocol (CoAP) (No. RFC 7252).
11. Sicari, S., Rizzardi, A., Grieco, L. A., &Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. Computer Networks, 76, 146-164.
12. Singh, D., Tripathi, G., &Jara, A. J. (2014). A survey of Internet-of-Things: Future vision, architecture, challenges and services. In IEEE World Forum on Internet of Things (WF-IoT) (pp. 287-292).