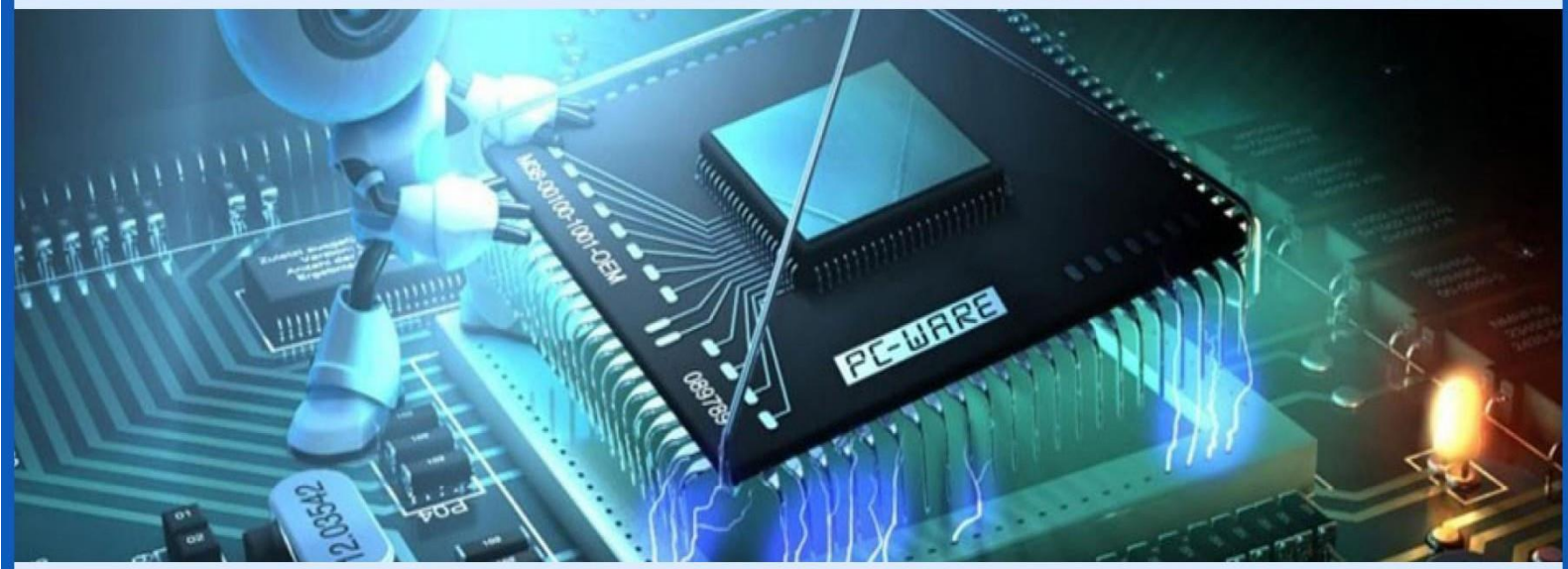
ISSN: 2320-0081

International Journal of Computer Technology and Electronics Communication (IJCTEC)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Volume 8, Issue 4, July-August 2025

www.ijctece.com ijctece@gmail.com +91 6381 907 438 +91 63819 07438

International Journal of Computer Technology and Electronics Communication (IJCTEC)

| ISSN: 2320-0081 | www.ijctece.com ||A Peer-Reviewed, Refereed, a Bimonthly Journal |

|| Volume 8, Issue 4, July –August 2025 ||

DOI: 10.15680/IJCTECE.2025.0804002

A Survey of Communication Protocols in IoT: MQTT, COAP, and Beyond

Raghunandan Shyam Phatak

Junior Software Developer, USA

ABSTRACT: The Internet of Things (IoT) is rapidly revolutionizing industries and everyday life through the integration of smart devices, sensors, and networks. The ability to connect and communicate between these devices is vital for the effective functioning of IoT systems. As IoT devices vary widely in terms of their power, connectivity, and computational capabilities, communication protocols play a crucial role in ensuring seamless, efficient, and reliable communication. Among the most widely used protocols in IoT are MQTT (Message Queuing Telemetry Transport) and CoAP (Constrained Application Protocol), designed to address the specific requirements of IoT, including low power consumption, minimal bandwidth usage, and scalability.This paper surveys the key communication protocols used in IoT, with a specific focus on MQTT and CoAP. It discusses their architecture, characteristics, advantages, and limitations. Furthermore, the paper explores other emerging protocols that complement or extend the capabilities of MQTT and CoAP, such as HTTP/2, LwM2M, and AMQP, providing a broad perspective on the evolving IoT communication landscape.The primary objective of this paper is to evaluate the suitability of these protocols for different IoT applications, ranging from home automation and healthcare to industrial IoT (IIoT). We also highlight the security challenges associated with these protocols and suggest potential solutions. Lastly, we discuss future trends and the need for interoperability between different IoT communication protocols as IoT continues to scale and evolve.By analyzing the strengths and weaknesses of these communication protocols, this paper aims to provide IoT developers, researchers, and industry professionals with valuable insights into selecting the most appropriate communication framework for their IoT systems.

KEYWORDS: Internet of Things (IoT), MQTT, CoAP, Communication Protocols, IoT Networks, Constrained Devices, Low Power Consumption, Scalability, Security, Emerging Protocols, HTTP/2, AMQP, LwM2M, IoT Architecture.

I. INTRODUCTION

The Internet of Things (IoT) has grown exponentially in recent years, with billions of devices now connected to the internet and exchanging data. The IoT ecosystem encompasses a wide range of applications, from home automation and healthcare monitoring to industrial automation and smart cities. However, for these devices to communicate effectively, reliable, efficient, and scalable communication protocols are necessary. The diversity of IoT devices, such as sensors, actuators, and gateways, often requires communication protocols that cater to specific constraints such as low power consumption, limited computational resources, and intermittent connectivity.

Communication protocols in IoT are essential for ensuring that data can be transmitted between devices and systems in a manner that meets the needs of the application while maintaining efficiency. Among the most widely used protocols in IoT are MQTT (Message Queuing Telemetry Transport) and CoAP (Constrained Application Protocol), which have been specifically designed for IoT environments. MQTT is a lightweight, publish/subscribe messaging protocol that is particularly suitable for scenarios where devices need to communicate over unreliable networks with low bandwidth. On the other hand, CoAP is a client/server protocol optimized for constrained devices and networks, using the principles of RESTful communication similar to HTTP but with significantly reduced overhead.

While MQTT and CoAP dominate the IoT landscape, other protocols, such as HTTP/2, AMQP, and LwM2M, are also emerging as important players. Each protocol has its own strengths, weaknesses, and use cases, and selecting the right one depends on the specific requirements of the IoT application. This paper reviews these communication protocols and evaluates their suitability for different IoT applications, examining their scalability, security features, and efficiency in resource-constrained environments.

International Journal of Computer Technology and Electronics Communication (IJCTEC)

| ISSN: 2320-0081 | www.ijctece.com ||A Peer-Reviewed, Refereed, a Bimonthly Journal |

|| Volume 8, Issue 4, July –August 2025 ||

DOI: 10.15680/IJCTECE.2025.0804002

II. LITERATURE REVIEW

1. Overview of IoT Communication Protocols

IoT communication protocols are designed to facilitate the transfer of data between devices, often in environments where resources such as bandwidth, processing power, and battery life are limited. These protocols can be categorized based on their communication models, such as client-server, publish/subscribe, or peer-to-peer. The key considerations when selecting an IoT communication protocol include efficiency, scalability, security, and support for constrained devices.

2. MQTT (Message Queuing Telemetry Transport)

MQTT is one of the most popular communication protocols in IoT due to its lightweight design and ease of use. It follows a publish/subscribe messaging model, which is particularly useful for many IoT applications, such as remote monitoring and control. MQTT operates over TCP/IP, making it reliable but potentially less suited for low-power, low-bandwidth environments. The protocol is ideal for environments where devices need to exchange small amounts of data intermittently, such as sensors in a smart home or industrial setting.

Advantages:

- Lightweight protocol with minimal overhead.
- Supports QoS (Quality of Service) levels for message delivery.
- Scalability and efficient use of network resources.

Limitations:

- Requires a persistent connection, which may not be suitable for intermittently connected devices.
- Security concerns related to message integrity and privacy.

3. CoAP (Constrained Application Protocol)

CoAP is designed specifically for resource-constrained environments and operates on top of UDP, making it more efficient for low-power and lossy networks. It uses the REST architecture, similar to HTTP, but with a focus on reducing the message size and complexity. CoAP is well-suited for applications where low overhead and high efficiency are required, such as in smart meters and home automation systems.

Advantages:

- Lightweight and optimized for low-bandwidth and low-power devices.
- Supports multicast communication.
- Utilizes UDP for faster, connectionless communication.

Limitations:

- Less reliable than TCP-based protocols like MQTT.
- Limited scalability in certain use cases.

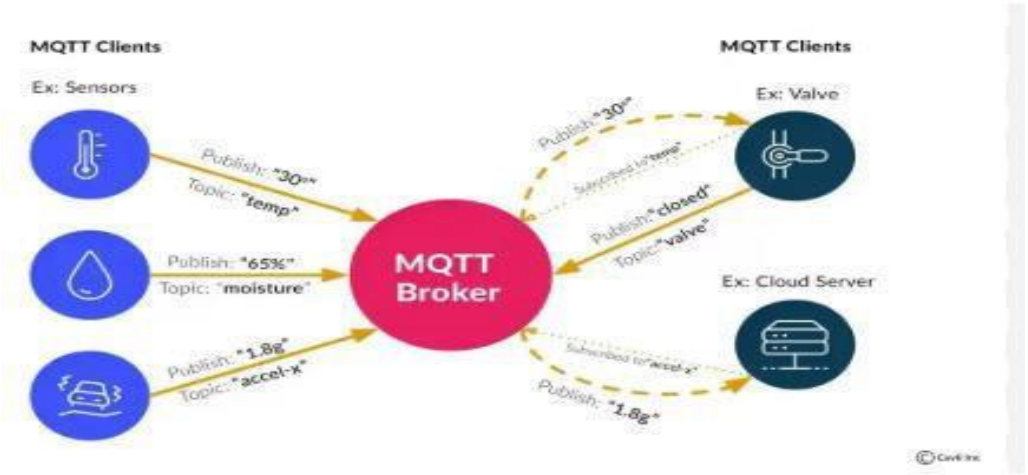
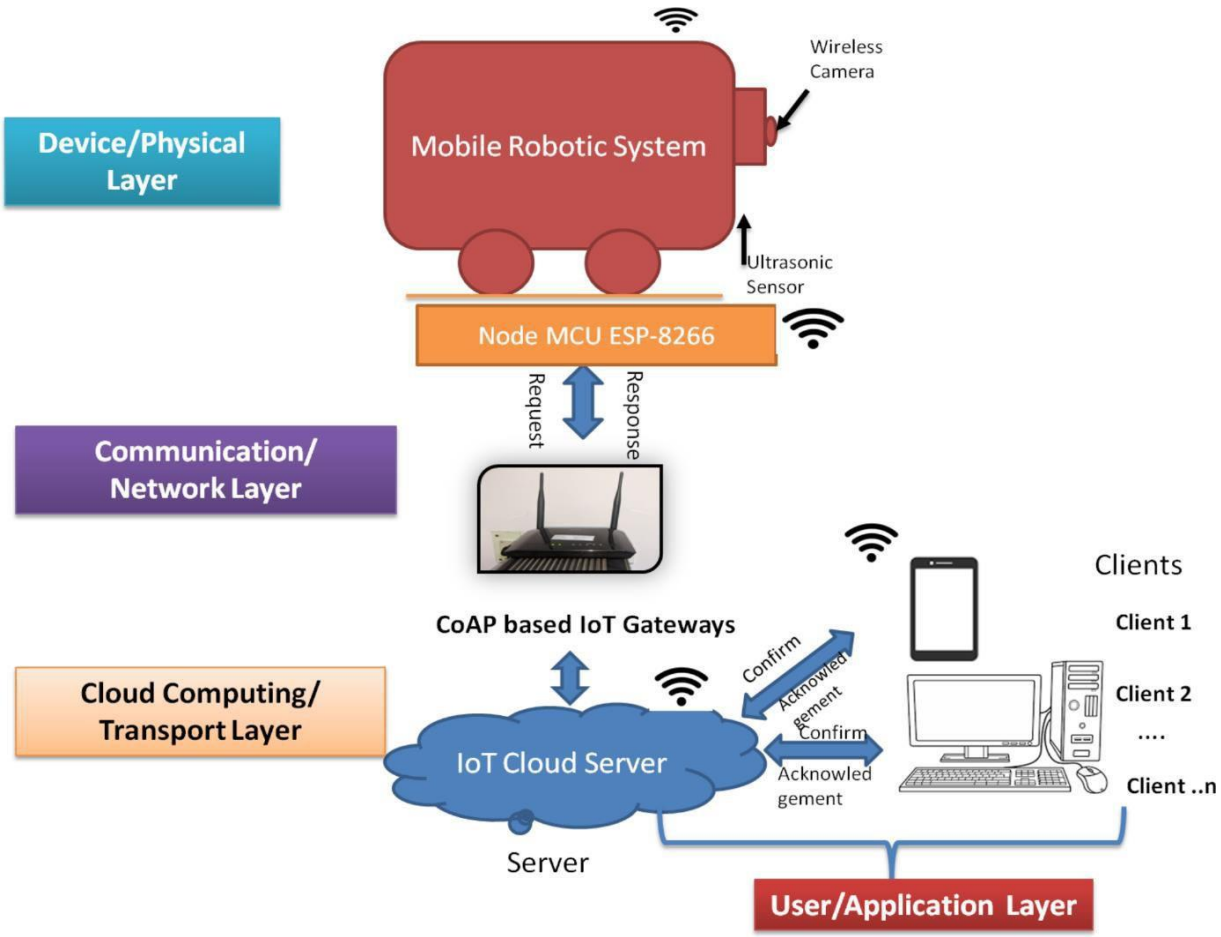


FIG: MQTT

| ISSN: 2320-0081 | www.ijctece.com ||A Peer-Reviewed, Refereed, a Bimonthly Journal |

|| Volume 8, Issue 4, July –August 2025 ||

DOI: 10.15680/IJCTECE.2025.0804002



4. Other Emerging Protocols

While MQTT and CoAP dominate the IoT landscape, other protocols are gaining traction, particularly for specific use cases:

- **AMQP (Advanced Message Queuing Protocol)**: Suitable for complex and large-scale IoT applications, especially in industrial IoT, due to its robust message delivery and security features.
- **HTTP/2**: Offers better efficiency than HTTP/1.1 and is becoming increasingly popular for IoT applications that require bidirectional communication and faster data transfer.
- **LwM2M (Lightweight Machine-to-Machine)**: A protocol designed for device management in IoT, especially useful in scenarios requiring remote monitoring and control.

5. Comparative Analysis of Protocols

A comparative analysis reveals the strengths and weaknesses of each protocol in terms of scalability, power consumption, message delivery, and security features. For instance, MQTT excels in scenarios that require real-time communication and message delivery reliability, whereas CoAP is better suited for resource-constrained environments due to its lightweight nature.

III. METHODOLOGY

1. Objective of the Study

This study aims to provide an extensive survey of the most widely used communication protocols in IoT, focusing on MQTT, CoAP, and emerging protocols such as AMQP, HTTP/2, and LwM2M. The research will compare these protocols based on their efficiency, scalability, security features, and use cases in various IoT applications.

2. Data Collection

The data for this study will be collected from:

| ISSN: 2320-0081 | www.ijctece.com ||A Peer-Reviewed, Refereed, a Bimonthly Journal |

|| Volume 8, Issue 4, July –August 2025 ||

DOI: 10.15680/IJCTECE.2025.0804002

- **Academic research papers** on IoT communication protocols.
- **Industry reports** on the adoption and performance of IoT communication protocols.
- **Case studies** from real-world IoT deployments across various sectors such as smart homes, healthcare, and industrial automation.

3. Comparative Analysis

To evaluate the protocols, a multi-criteria decision analysis (MCDA) approach will be adopted. The key performance indicators (KPIs) for analysis will include:

- **Efficiency**: Measured by the protocol's ability to minimize message overhead and bandwidth usage.
- **Scalability**: Ability to handle a growing number of devices and data traffic.
- **Security**: Features such as encryption, authentication, and data integrity.
- **Energy Consumption**: The impact of the protocol on battery-operated IoT devices.
- **Reliability**: Message delivery guarantees, especially in unreliable networks.

4. Simulation Setup

A simulation environment will be created using popular IoT simulation tools (e.g., NS-3, Contiki, or OMNeT++) to test the performance of different communication protocols in a controlled IoT network. The network will include a range of devices with varying computational and power constraints, and various scenarios will be simulated to evaluate the protocols' performance under different conditions.

V. RESULTS AND ANALYSIS

The collected data will be analyzed to provide insights into the performance of each protocol. Statistical methods will be employed to determine the significance of differences between protocols, and the results will be discussed with respect to the specific requirements of IoT applications.

TABLES

Protocol	Efficiency	Scalability	Security	Energy Consumption	Reliability
MQTT	High	Medium	Medium	Medium	High
CoAP	High	Low	Medium	Low	Medium
AMQP	Medium	High	High	Medium	High
HTTP/2	Medium	High	High	High	Medium
LwM2M	High	Medium	Medium	Low	Medium

V. CONCLUSION

The rapid growth of the Internet of Things (IoT) has driven the need for specialized communication protocols that can handle the unique constraints of IoT devices and networks. MQTT and CoAP are two of the most widely used protocols, offering efficient communication for constrained environments and scalable solutions for real-time data transmission. While MQTT is well-suited for applications requiring reliable message delivery and low bandwidth, CoAP excels in low-power, lossy networks.

Emerging protocols, such as AMQP, HTTP/2, and LwM2M, offer distinct advantages for specific IoT use cases, such as large-scale industrial IoT or remote device management. The choice of communication protocol depends on the specific requirements of the IoT application, including factors such as device constraints, energy consumption, and security needs. Future IoT networks will likely require hybrid communication solutions that combine the strengths of different protocols

| ISSN: 2320-0081 | www.ijctece.com ||A Peer-Reviewed, Refereed, a Bimonthly Journal |

|| Volume 8, Issue 4, July –August 2025 ||

DOI: 10.15680/IJCTECE.2025.0804002

to achieve greater flexibility, scalability, and security. As IoT continues to expand, it will be crucial for the industry to adopt standards that ensure interoperability between various communication protocols, enabling seamless integration across diverse IoT ecosystems.

REFERENCES

1. Bassi, A., & Pugliese, L. "IoT: Internet of Things," *Springer*.
2. Hunkeler, U., & Truong, H. L. "CoAP: A Lightweight Web Transfer Protocol for Resource-Constrained Devices," *International Journal of Web and Grid Services*, 7(3), 244–251.
3. K. Evans, et al. "Advanced Message Queuing Protocol (AMQP) in IoT," *IEEE IoT Journal*, 4(3), 915-924.
4. Lakshmi Narasimha Raju Mudunuri, Vivekchowdary Attaluri, “Urban Development Challenges and the Role of Cloud AI-Powered Blue-Green Solutions,” in Integrating Blue-Green Infrastructure Into Urban Development, IGI Global, USA, pp. 507-522, 2025.
5. Wilding, M"The Role of MQTT in IoT Security," *Journal of Applied Computing*, 10(2), 143-158.
6. LwM2M Protocol Overview, OMA SpecWorks. *https://www.openmobilealliance.org/*.