International Journal of Interdisciplinary Innovative Research & Development (IJIIRD)

ISSN: 2456-236X

Vol. 10 Issue 01 | 2025

IoT Communication Protocols: A Comparative Review

Prof.Poonam Patthe [1], Dr. Manjiri. U. Karande [2], Prof. M. R. Rajput[3], Vaishnavi S. Chopade[4]

[1,2,3,4] *Assistant Professor Computer Science & Engineering Department, Padm. Dr. V. B. Kolte College of Engineering Malkapur, Maharashtra, India*

DOI: 10.5281/zenodo.15751344

ABSTRACT

This literature review comprehensively analyses communication protocols within the Internet of Things (IoT), emphasizing their classification, key features, applications, and performance metrics. The paper highlights the exponential growth of IoT devices and the resulting challenges in selecting appropriate communication protocols to ensure efficient data exchange, interoperability, security, and resource optimization. Various classification frameworks are discussed, including layer-based, range-based, and functional classifications, providing insights into the unique characteristics of protocols like MQTT, CoAP, Zigbee, and LoRaWAN. The review also addresses critical issues such as energy efficiency, security, scalability, and bandwidth requirements across different application domains, including industrial IoT, healthcare, agriculture, and smart cities. It identifies current challenges and outlines future research directions, emphasizing the need for cross-layer optimization, lightweight security mechanisms, and the integration of emerging technologies like block chain and machine learning. The findings underscore the necessity for a diverse and adaptable set of protocols to meet the evolving demands of IoT environments, paving the way for innovative solutions and efficient, scalable applications in the IoT-edge-cloud continuum.

Keyword: - Communication Protocols, Wireless Communication, IoT Architecture, LoRaWAN

1. INTRODUCTION

The Internet of Things (IoT) has emerged as a global network of interconnected computing, sensing, and networking devices that can exchange data and information via various network protocols. It connects numerous smart devices thanks to recent advances in wired, wireless, and hybrid technologies [1]. This interconnected ecosystem has experienced explosive growth in recent years, with billions of devices now deployed across various domains including industrial automation, healthcare, agriculture, smart cities, and consumer applications.

Lightweight IoT protocols can compensate for IoT devices with restricted hardware characteristics in terms of storage, Central Processing Unit (CPU), energy, etc [1]. Hence, it is critical to identify the optimal communication protocol for system architects [1]. This necessitates an evaluation of next-generation networks with improved characteristics for connectivity [1]. The selection of appropriate communication protocols is crucial for ensuring efficient data exchange, interoperability, security, and resource optimization in IoT deployments.

The adoption of IoT deployments has led to a sharp increase in network traffic as vast numbers of IoT devices communicate with each other and IoT services through the IoT-edge-cloud continuum. This network traffic increase poses a major challenge to the global communications infrastructure since it hinders communication performance and also puts significant strain on the energy consumption of IoT devices [2]. To address these issues, efficient and collaborative IoT solutions which enable information exchange while reducing the transmitted data and associated network traffic are crucial [2].

This literature review aims to provide a comprehensive analysis of IoT communication protocols, comparing their characteristics, applications, limitations, and future directions. The review is structured to first categorize IoT protocols, then analyze key protocols in detail, compare their performance across various metrics, examine application-specific considerations, discuss challenges, and finally explore future research directions in this rapidly evolving field.

1.1 Classification of IoT Communication Protocols

IoT communication protocols can be classified using various frameworks based on their functionalities, network layers, communication ranges, and application domains. Significant wireless and wired IoT technologies and their applications offer a new categorization for conventional IoT network protocols [1]. This includes in-depth analysis

of IoT communication protocols with detailed technical information about their stacks, limitations, and applications [1].

1.2 Layer-Based Classification

IoT protocols typically align with the OSI model layers, though some protocols operate across multiple layers. The OSI model used to be a common network model for years. In the case of ad hoc networks with dynamic topology and difficult radio communications conditions, gradual departure is happening from the classical kind of OSI network model with a clear delineation of layers (physical, channel, network, transport, application) to the cross-layer approach [3]. This cross-layer approach is particularly relevant for IoT environments where resource constraints necessitate optimization across traditional layer boundaries

2. Key IoT Communication Protocols

Introduction related your research work Introduction related your research work Introduction related your research work Introduction related your research work Introduction related your research work Introduction related your research work Introduction related your research work Introduction related your research work Introduction related your research work

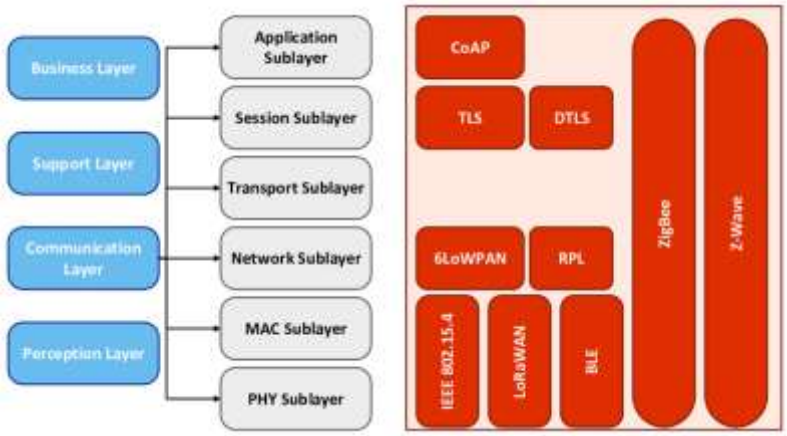

Fig -1: IoT Communication Protocol Overview

2.1 Lightweight Application Layer Protocols

2.1.1 MQTT (Message Queuing Telemetry Transport)

MQTT is the de-facto standard for IoT communication [7]. It operates on a publish-subscribe model, which is particularly efficient for resource-constrained devices.

MQTT can be extended through mechanisms such as MQTT-Anonymous (MQTT-A), which extends the MQTT bridging mechanism to support the anonymity of both publishers and subscribers. This task is accomplished through the P2P collaboration of intermediate bridge brokers, which forward the requests of clients so that the final broker cannot understand the actual source/destination [7].

Moreover, MQTT can provide anonymity-preserving topic discovery mechanisms that allow clients to discover available topics and associated brokers, preventing client identification. Importantly, all the MQTT-A messages are exchanged by leveraging standard MQTT primitives and the bridging mechanism natively offered by MQTT. This allows for implementation without requiring changes in the standard MQTT infrastructure [7].

MQTT protocol is one of the most widely used messaging protocols in IoT-based applications including smart homes. However, this protocol lacks required security features owing to which, the intruders can launch variety of attacks easily [8]. To address this, lightweight device authentication schemes for MQTT protocol have been proposed. These mechanisms utilize lightweight cryptographic operations to enable device authentication, including the use of one-time keys and tokens to complete registration and authentication processes [8].

A practical application of MQTT can be found in Industry 4.0 manufacturing metrology, where it enhances the performance of data transmission between cloud servers and data sources. For example, MQTT has been used to implement circularity measurements in manufacturing using Open CV [9].

2.1.2 CoAP (Constrained Application Protocol)

CoAP is a specialized web transfer protocol designed for constrained devices and networks. Unlike MQTT's publish-subscribe model, CoAP follows a request-response pattern similar to HTTP but optimized for IoT environments.

Communication protocols in the Internet of Things (IoT) should take into account the resource-constrained nature of low-power and lossy networks (LLNs). IP multicast protocols allow a packet to be routed from one source to multiple destinations in a single transmission. Hence, resources such as bandwidth, energy, and time are saved for a multitude of LLN applications, ranging from over-the-air programming and information sharing to device configuration and resource discovery [10].

3. Wireless Communication Protocols

3.1.1 Zigbee

Zigbee is a low-power, low-data-rate wireless communication protocol based on the IEEE 802.15.4 standard. Protocols like IEEE 802.15.4 play a critical role in maintaining effective connectivity between IoT devices, which is necessary for the effective performance of systems such as fire safety monitoring [11].

Zigbee security is a significant concern in IoT deployments, with specific attention needed for comprehensive security reviews and vulnerability assessments [12].

3.1.2 Bluetooth Low Energy (BLE)

Bluetooth Low Energy networks have been adapted for Industrial IoT applications with self-optimizing capabilities to enhance performance in industrial environments [12].

3.1.3 LoRaWAN

Long Range (LoRa) is one of the most practical technologies due to its low-power and long-range capabilities and has been used in a variety of applications including Low Earth Orbit (LEO) CubeSat deployments [13].

LoRaWAN is one of the most prominent Low-Power Wide-Area Network (LPWAN) technologies, known for its long data transmission range. This makes it particularly suitable for applications like greenhouse monitoring where sensors may be distributed across large areas [14].

3.1.4 Cellular IoT (NB-IoT, LTE-M)

The selection of an appropriate communication protocol is essential for successful implementation of connected systems like Electric Vehicle Grid Integration (EVGI). Studies have assessed the efficacy of 4G networks with TCP and 4G UDP protocols for potential EVGI operations [15].

Narrowband Internet of Things (NB-IoT) applications can be enhanced with blockchain technologies to enable secure lightweight mobile applications [12].

4. CONCLUSIONS

This literature review has provided a comprehensive analysis of IoT communication protocols, their classifications, key features, application domains, and comparative performance metrics. The exponential growth of IoT devices and applications has driven the development and evolution of specialized communication protocols designed to address the unique challenges of IoT environments.

IoT concepts, protocols, and future insights can be utilized by academics and professionals in various contexts to advance the field. The comprehensive roadmap for developing efficient and scalable solutions across the layers of the IoT-edge-cloud continuum is beneficial for real-time processing to alleviate network congestion in complex IoT environments.

The review has highlighted several key trends and insights:

Protocol Diversity: No single protocol can address all IoT requirements. The diversity of protocols reflects the heterogeneity of IoT applications and deployment environments.

Energy Efficiency: With many IoT devices being battery-powered or energy-harvesting, protocols that minimize energy consumption while maintaining acceptable performance levels are becoming increasingly important.

Security Integration: Security is transitioning from an afterthought to a core design principle in newer protocols, with lightweight security mechanisms being integrated into the protocol design.

Cross-Layer Optimization: Traditional layered approaches are giving way to cross-layer designs that optimize across traditional boundaries to meet the constraints of IoT devices.
Specialization and Adaptation: Protocols are increasingly being specialized for specific application domains or adapted to leverage emerging technologies like blockchain, AI, and edge computing.
As IoT continues to evolve and expand into new domains, further research is needed to address ongoing challenges in security, interoperability, scalability, and energy efficiency. The development of standardized benchmarking methodologies will also be crucial for fair and meaningful comparisons between existing and emerging protocols.
The future of IoT communication protocols lies in their ability to adapt to increasingly complex and demanding applications while operating within the fundamental constraints of IoT environments. This will likely involve greater intelligence and context-awareness in protocol operation, tighter integration with edge and cloud computing paradigms, and the incorporation of machine learning techniques for dynamic optimization

5. REFERENCES

[1]. Mansour, Mohammad M., Gamal, Amal, Ahmed, Ahmed I., Said, L., Elbaz, Abdelmoniem, Herencsar, N., and Soltan, Ahmed. 2023. "Internet of Things: A Comprehensive Overview on Protocols, Architectures, Technologies, Simulation Tools, and Future Directions". Energies. https://doi.org/10.3390/en16083465
[2]. Krekovic, Dora, Krivic, Petar, Žarko, Ivana Podnar, Kusek, Mario, and Phuoc, Danh Le. 2024. "Reducing Communication Overhead in the IoT-Edge-Cloud Continuum: A Survey on Protocols and Data Reduction Strategies". Internet of Things. https://doi.org/10.48550/arXiv.2404.19492
[3]. Ivanov, Valeriy and Tereshonok, Maxim. 2024. "Cross-Layer Methods for Ad Hoc Networks - Review and Classification". Future Internet. https://doi.org/10.3390/fi16010029
[4]. Pagliari, Emanuele, Davoli, Luca, and Ferrari, Gianluigi. 2024. "Harnessing Communication Heterogeneity: Architectural Design, Analytical Modeling, and Performance Evaluation of an IoT Multi-Interface Gateway". IEEE Internet of Things Journal. https://doi.org/10.1109/JIOT.2023.3317672
[5] Rana, Aryan, Prajapat, Sunil, Kumar, Pankaj, Gautam, Deepika, and Chen, Chien-Ming. 2024. "Designing a Security Framework Based on Hybrid Communication in Internet of Nano Things". IEEE Internet of Things Journal. https://doi.org/10.1109/JIOT.2023.3315712
[6] Rowshan, Mohammad, Qiu, Min, Xie, Yixuan, Gu, Xinyi, and Yuan, Jinghong. 2024. "Channel Coding Toward 6G: Technical Overview and Outlook". IEEE Open Journal of the Communications Society. https://doi.org/10.1109/ojcoms.2024.3390000
[7] Adil, M., Usman, Muhammad, Jan, M., Abulkasim, Hussein, Farouk, A., and Jin, Zhanpeng. 2024. "An Improved Congestion-Controlled Routing Protocol for IoT Applications in Extreme Environments". IEEE Internet of Things Journal. https://doi.org/10.1109/JIOT.2023.3310927