The OSCAR PUBLISHING Services
American Journal of Applied Science and Technology

VOLUME Vol.05 Issue 04 2025
PAGE NO. 106-110

Communication Protocols, Energy Efficiency, Security, and Sustainability Trade-offs in Internet of Things Architectures: A Comprehensive Theoretical and Empirical Synthesis

Dr. Jonathan R. Whitmore
Department of Computer Science and Engineering Northbridge University, United Kingdom

Received: 01 April 2025; **Accepted:** 15 April 2025; **Published:** 30 April 2025

Abstract: The Internet of Things has become a foundational paradigm in contemporary digital transformation, enabling large-scale interconnection between physical objects and cyber systems across domains such as smart cities, healthcare, industrial automation, energy systems, and environmental monitoring. At the core of IoT functionality lie communication and messaging protocols that govern data exchange among heterogeneous, resource-constrained, and often energy-limited devices. The selection and integration of these protocols have profound implications for system performance, scalability, energy efficiency, security, and long-term sustainability. Despite extensive research, the existing literature remains fragmented across protocol-specific studies, high-level surveys, industry adoption reports, and emerging discussions on energy-aware and secure IoT systems. This article presents a comprehensive, publication-ready research synthesis strictly grounded in established academic references and authoritative industry sources. Through extensive theoretical elaboration and comparative analysis, the study examines enabling technologies, application-layer messaging protocols, protocol overhead, energy consumption characteristics, security challenges, and sustainability considerations in IoT architectures. The methodology is qualitative and analytical, emphasizing cross-study synthesis rather than experimental benchmarking. The findings demonstrate that no single protocol optimally satisfies all IoT requirements; instead, protocol suitability is determined by application context, device constraints, network topology, and security needs. The discussion highlights persistent trade-offs, methodological limitations in existing studies, and the growing importance of energy-aware and secure design principles. The article concludes by outlining future research directions focused on unified evaluation frameworks, adaptive protocol stacks, and sustainable IoT system design.

Keywords: Internet of Things, communication protocols, MQTT, CoAP, energy efficiency, IoT security, sustainability

Introduction

The Internet of Things represents a transformative evolution in computing and communication, extending the reach of the Internet beyond traditional endpoints to encompass billions of physical objects embedded with sensing, processing, and communication capabilities. These objects, commonly referred to as “things,” interact with their environment and with each other to enable data-driven automation, monitoring, and decision-making across diverse application domains (Al-Fuqaha et al., 2015). Unlike conventional computing systems, IoT environments are characterized by extreme heterogeneity, large-scale distribution, intermittent connectivity, and stringent resource constraints. These characteristics fundamentally challenge traditional assumptions about network design, protocol efficiency, and system security.

One of the most critical design decisions in any IoT system concerns the choice of communication and messaging protocols. These protocols define how data is formatted, transmitted, acknowledged, and protected as it moves across networks. Early IoT implementations frequently relied on adaptations of conventional Internet protocols, particularly HTTP operating over TCP/IP. While this approach benefited from widespread familiarity and mature tooling, it quickly proved inadequate for many IoT scenarios due to excessive overhead, synchronous communication

patterns, and inefficient energy usage (Naik, 2017).

In response, a new generation of lightweight and specialized IoT protocols emerged, including MQTT, CoAP, and AMQP. These protocols were designed to address the unique requirements of constrained devices and lossy networks, emphasizing minimal overhead, asynchronous communication, and flexible interaction models (Chaudhary et al., 2017). However, the proliferation of protocols has introduced new complexity into IoT system design, making protocol selection a non-trivial and context-dependent problem.

Beyond performance considerations, energy efficiency has become a central concern in IoT research and practice. Many IoT devices operate on batteries or energy-harvesting mechanisms and are expected to function for years without maintenance. Communication activities often dominate energy consumption, surpassing sensing and computation in many deployments (Anusha et al., 2017). As a result, protocol design and configuration play a decisive role in determining device lifetime and operational sustainability.

Security further complicates this landscape. IoT devices are increasingly targeted by cyberattacks that exploit weak authentication, insufficient encryption, and limited update mechanisms. Lightweight protocols, while efficient, often struggle to support robust security features due to constrained computational resources (Mahamat et al., 2023). Industry analyses emphasize that security breaches in IoT systems can have far-reaching consequences, including privacy violations, service disruptions, and physical safety risks (Onomondo, 2025).

More recently, sustainability has emerged as a broader framing for IoT system evaluation. The cumulative environmental impact of billions of devices, their communication infrastructures, and supporting cloud services has prompted renewed attention to energy-aware design and lifecycle considerations (MicroEJ, 2022). From this perspective, communication protocols are not merely technical components but contributors to global energy consumption and carbon emissions.

Despite a rich body of literature, existing research often treats communication efficiency, energy consumption, and security as separate concerns. Surveys and comparative studies provide valuable insights but rarely integrate these dimensions into a unified analytical framework (Dizdarevic et al., 2019). Furthermore, discrepancies between academic evaluations and industry adoption trends highlight the influence of non-technical factors such as ecosystem maturity and developer familiarity (Eclipse Foundation, 2018; 2019; 2020).

This article addresses these gaps by presenting a comprehensive synthesis of IoT communication protocols and their implications for energy efficiency, security, and sustainability. Strictly grounded in the provided references, the study emphasizes deep theoretical elaboration, critical comparison, and architectural interpretation. The objective is not to propose new protocols but to advance conceptual understanding and inform future research and system design.

Methodology

The methodological approach of this study is qualitative, analytical, and synthesis-driven. Given the objective of producing a comprehensive and publication-ready research article based strictly on existing references, the methodology does not involve experimental deployments, simulations, or numerical modeling. Instead, it relies on systematic examination, comparison, and interpretation of peer-reviewed journal articles, conference proceedings, industry surveys, and authoritative technical documentation.

The first stage of the methodology involved organizing the reference material into thematic categories. These categories include foundational IoT architectures and enabling technologies, application-layer messaging protocols, protocol performance and overhead considerations, developer adoption trends, energy efficiency and sustainability, and security challenges in constrained environments. This thematic structuring enabled a coherent analytical narrative while preserving the interconnections among different research dimensions.

Within each category, the analysis focused on identifying underlying assumptions, design goals, and reported findings. For example, protocol surveys were examined not only for descriptive comparisons but also for the criteria used to evaluate performance, such as latency tolerance, reliability requirements, and scalability expectations (Dizdarevic et al., 2019). Industry surveys conducted by the Eclipse Foundation were analyzed longitudinally to understand how protocol adoption evolved over time and how practical considerations influenced developer choices (Eclipse Foundation, 2018; 2019; 2020).

Comparative reasoning constituted a central methodological principle. Rather than ranking protocols based on isolated metrics, the study emphasized trade-offs and contextual suitability. Messaging models, transport-layer dependencies, and security mechanisms were analyzed in relation to specific application scenarios, such as cloud-centric data aggregation versus local device-to-device interaction (Naik, 2017).

Energy efficiency considerations were examined through qualitative interpretation of studies on protocol overhead, transmission behavior, and embedded system design. Insights from energy benchmarking research, including work on distributed embedded communication architectures, were incorporated to enrich the discussion on synchronization, reliability, and power stability (Abdul, 2024; Gutiérrez Hermosillo Muriedas et al., 2023). Although some of these studies originate outside traditional IoT contexts, their conceptual frameworks provide valuable perspectives on systematic energy awareness.

Security analysis drew on both academic surveys and industry-focused discussions to capture theoretical vulnerabilities and practical mitigation strategies. This dual perspective ensured that the discussion reflects both formal research findings and real-world operational challenges (Mahamat et al., 2023; Onomondo, 2025).

Throughout the methodological process, strict adherence to the provided references was maintained. No external sources, speculative claims, or undocumented data were introduced. Each major analytical claim is supported by in-text citations, ensuring academic rigor and traceability. The result is an integrative synthesis that bridges fragmented strands of existing research into a cohesive conceptual framework.

Results

The synthesis of the referenced literature yields several consistent and significant findings regarding IoT communication protocols and their broader architectural implications. One of the most prominent outcomes is the reaffirmation that protocol diversity is both inevitable and necessary in the IoT ecosystem. Surveys consistently emphasize that the heterogeneity of devices, networks, and applications precludes the existence of a universally optimal communication protocol (Al-Fuqaha et al., 2015; Dizdarevic et al., 2019).

Application-layer messaging protocols such as MQTT and CoAP emerge as dominant solutions for constrained environments, yet their strengths and limitations differ markedly. MQTT's publish-subscribe paradigm, operating over TCP, offers reliable message delivery and temporal decoupling between publishers and subscribers. These characteristics make it particularly well suited for cloud-integrated IoT applications and large-scale data aggregation scenarios (Naik, 2017; MQTT.org). However, the maintenance of persistent connections and acknowledgment mechanisms introduces additional overhead and energy consumption, especially in scenarios involving intermittent connectivity.

CoAP, by contrast, adopts a request-response model over UDP, emphasizing minimal overhead and simplicity. Its design aligns closely with RESTful principles while accommodating the constraints of low-power networks (Chaudhary et al., 2017). Optional reliability mechanisms and observe extensions enable asynchronous communication, but their configuration complexity can offset theoretical efficiency gains. Comparative overhead analyses suggest that while CoAP messages are generally smaller, overall energy consumption depends heavily on retransmission behavior and security layer integration (Sarafov, 2018).

Developer adoption trends, as reflected in Eclipse Foundation surveys, reveal the importance of ecosystem factors. MQTT consistently ranks among the most widely adopted protocols, reflecting its maturity, extensive tooling support, and seamless integration with major cloud platforms (Eclipse Foundation, 2018; 2019; 2020). CoAP, despite its technical suitability for constrained devices, exhibits more limited adoption, suggesting that developer familiarity and platform support significantly influence real-world protocol selection.

Energy efficiency emerges as a critical cross-cutting result. Studies indicate that communication activities often dominate energy consumption in IoT devices, making protocol efficiency a key determinant of device lifetime (Anusha et al., 2017). Protocol overhead, message frequency, and connection management strategies collectively influence power usage. Research on distributed embedded communication architectures further highlights that synchronization accuracy and skew management can affect power stability and efficiency, particularly in large-scale and safety-critical systems (Abdul, 2024).

Security analyses reveal persistent vulnerabilities associated with constrained devices and lightweight protocols. Many IoT attacks exploit insufficient authentication, weak encryption, or poor key management (Mahamat et al., 2023). Industry analyses emphasize that while lightweight protocols may rely on simplified security mechanisms, overall system security depends on architectural integration with gateways, device management services, and cloud platforms (Onomondo, 2025).

Collectively, these results underscore that protocol evaluation cannot be reduced to isolated performance metrics. Instead, effective IoT system design requires a holistic understanding of trade-offs across performance, energy efficiency, security, and ecosystem compatibility.

Discussion

The findings of this study invite a deeper discussion of the theoretical and practical implications of communication protocol selection in IoT architectures. At a theoretical level, the observed diversity of protocols reflects fundamental trade-offs inherent in distributed systems design. The impossibility of optimizing all desirable properties simultaneously—such as low latency, high reliability, minimal energy consumption, and strong security—necessitates context-specific compromises.

One important implication concerns abstraction and middleware. Many contemporary IoT platforms adopt layered architectures that abstract protocol differences behind unified interfaces. While this approach enhances flexibility and developer productivity, it can obscure underlying communication behavior and hinder fine-grained energy optimization (Dizdarevic et al., 2019). Greater transparency and configurability may be required to align application-level requirements with protocol-level behavior.

Energy efficiency discussions highlight the need to consider system-level interactions rather than isolated protocol characteristics. A protocol with minimal message overhead may still incur significant energy costs if it requires frequent retransmissions or complex security negotiations. Conversely, protocols with higher per-message overhead may achieve better energy efficiency through reduced transmission frequency or more reliable delivery. Research on synchronization and skew management in distributed embedded systems reinforces the importance of low-level communication design for power stability and long-term efficiency (Abdul, 2024).

Security remains a particularly challenging domain. While lightweight protocols are often criticized for limited security features, the literature suggests that security should be viewed as an architectural property rather than a protocol-specific attribute. Gateways, authentication services, and lifecycle management mechanisms all contribute to the effective security posture of an IoT system (Mahamat et al., 2023). Industry perspectives emphasize the need for security solutions tailored to low-power devices, balancing cryptographic strength with computational feasibility (Onomondo, 2025).

The discussion also reveals limitations in existing research. Comparative protocol studies often rely on simplified experimental setups or specific hardware platforms, limiting the generalizability of their conclusions (Sarafov, 2018). Developer surveys, while valuable, reflect subjective perceptions and may lag behind emerging technological developments. Additionally, sustainability considerations are still relatively underrepresented in protocol evaluation frameworks, despite their growing importance (MicroEJ, 2022).

Future research should aim to address these limitations by developing unified evaluation methodologies that integrate performance, energy, security, and sustainability metrics. Adaptive protocol stacks capable of dynamically adjusting behavior based on context and resource availability represent a promising direction. Closer collaboration between academia and industry is also essential to ensure that theoretical advances translate into practical and sustainable IoT solutions.

Conclusion

This article has presented a comprehensive and integrative analysis of communication protocols in Internet of Things architectures, strictly grounded in established academic and industry references. Through extensive theoretical elaboration and comparative synthesis, the study has demonstrated that protocol selection is a multidimensional decision shaped by application requirements, device constraints, energy considerations, security needs, and ecosystem dynamics.

The findings reaffirm that no single protocol can address the diverse and evolving demands of IoT systems. Instead, effective design requires a nuanced understanding of trade-offs and, in many cases, the adoption of hybrid or adaptive communication strategies. Energy efficiency and sustainability emerge as critical considerations that must be incorporated into protocol evaluation and architectural planning from the outset. Security, while constrained by limited device resources, demands holistic and context-aware solutions.

By identifying gaps and limitations in existing research, this work provides a foundation for future investigations aimed at developing more coherent, energy-aware, and secure IoT communication frameworks. As IoT continues to expand in scale and societal impact, such integrative and theoretically grounded analyses will be essential for guiding both research and practice.

References

1. Abdul, A. S. (2024). Skew variation analysis in distributed battery management systems using CAN FD and chained SPI for 192-cell architectures. Journal of Electrical Systems, 20(6s), 3109–3117.
2. 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.

3. Anusha, M., Babu, E., Reddy, L. M., Krishna, A., & Bhagyasree, B. (2017). Performance analysis of data protocols of internet of things: A qualitative review. International Journal of Pure and Applied Mathematics, 115(6), 37–47.
4. Chaudhary, A., Peddoju, S. K., & Kadarla, K. (2017). Study of internet-of-things messaging protocols used for exchanging data with external sources. Proceedings of the IEEE International Conference on Mobile Ad Hoc and Sensor Systems, 666–671.
5. Dizdarevic, J., Carpio, F., Jukan, A., & Masip-Bruin, X. (2019). A survey of communication protocols for internet of things and related challenges of fog and cloud computing integration. ACM Computing Surveys, 51(6), 1–29.
6. Eclipse Foundation. (2018). IoT developer survey results.
7. Eclipse Foundation. (2019). IoT developer survey results.
8. Eclipse Foundation. (2020). IoT developer survey results.
9. Gutiérrez Hermosillo Muriedas, J. P., Flügel, K., Debus, C., Obermaier, H., Streit, A., & Götz, M. (2023). Perun: Benchmarking energy consumption of high-performance computing applications. In Euro-Par 2023: Parallel Processing.
10. Mahamat, M., Jaber, G., & Bouabdallah, A. (2023). Achieving efficient energy-aware security in IoT networks: A survey of recent solutions and research challenges. Wireless Networks, 29, 787–808.
11. MicroEJ. (2022). IoT and sustainability—How IoT and embedded systems impact global carbon emissions.
12. MQTT.org. MQTT.
13. Naik, N. (2017). Choice of effective messaging protocols for IoT systems: MQTT, CoAP, AMQP and HTTP. Proceedings of the IEEE International Systems Engineering Symposium.
14. Onomondo. (2025). IoT security issues and solutions for low-power devices.
15. Sarafov, V. (2018). Comparison of IoT data protocol overhead. Proceedings of the Seminars of Future Internet and Innovative Internet Technologies and Mobile Communication.