International Journal of Cyber Threat Intelligence and Secure Networking (IJCTISN)
eISSN: 3087-4297
Volume03 Issue08 | Page No: - 13-19

Received: 27 May 2026, Revised: 18 June 2026, Accepted: 28 July 2026, Published: 05 August 2026

DOI: https://doi.org/10.55640/ijctisn-v03i08-03

Cross-Layer Protocol Design and Integration Strategies for IoT and IoRT Convergence: An Analytical Review of Enabling Technologies, Challenges, and Emerging Solutions

Dr. Nguyen Van Minh[1], Dr. Tran Thi Lan[2]

[1] Faculty of Information Technology Hanoi University of Science and Technology, Hanoi, Vietnam

[2] Department of Cyber Security Vietnam National University, Ho Chi Minh City, Vietnam

ABSTRACT: The convergence of the Internet of Things (IoT) and the Internet of Robotic Things (IoRT) has introduced a complex heterogeneous ecosystem where sensing, communication, computation, and actuation are tightly interdependent. Traditional layered networking models are increasingly insufficient to support the stringent requirements of latency-sensitive, resource-constrained, and mobility-intensive robotic and IoT environments. This paper presents a comprehensive analytical review of cross-layer protocol design and integration strategies aimed at enabling seamless IoT–IoRT interoperability. It synthesizes existing architectural models, communication protocols, and enabling technologies, highlighting their strengths and limitations in supporting distributed intelligent systems. The study further examines protocol heterogeneity, energy efficiency constraints, reliability issues, and security vulnerabilities in integrated IoT–IoRT deployments. Drawing from established IoT architectures (Atzori et al., 2010; Gubbi et al., 2013), protocol surveys (Al-Sarawi et al., 2017; Sethi and Sarangi, 2017), and robotic IoT extensions (Ray, 2017), the paper identifies critical gaps in cross-layer optimization, adaptive routing, and real-time coordination. The analysis is reinforced by security and attack surface considerations highlighted in IoT systems (Bilal, 2017). The paper concludes by proposing an integrated conceptual framework for cross-layer protocol harmonization to support scalable and resilient IoT–IoRT ecosystems.

KEYWORDS: IoT, IoRT, cross-layer design, communication protocols, interoperability, robotic systems, network architecture, edge computing, protocol optimization, distributed systems.

1. Introduction

1.1 Background

The Internet of Things (IoT) has evolved into a global paradigm enabling interconnected smart devices to sense, communicate, and exchange data across heterogeneous networks. Early conceptualizations of IoT emphasized device interconnectivity and service-oriented architectures (Atzori et al., 2010), while later works expanded the domain into architectural layering, scalability challenges, and application diversity (Gubbi et al., 2013). Parallel to this evolution, the Internet of Robotic Things (IoRT) has emerged as an extension where autonomous robotic systems are integrated with IoT infrastructures to enable real-time perception, decision-making, and actuation in dynamic environments (Ray, 2017).

Unlike traditional IoT nodes, IoRT systems introduce stringent constraints such as real-time responsiveness, mobility awareness, and high computational coordination requirements. These differences fundamentally challenge conventional layered networking models, which typically isolate physical, link, network, transport, and application layers. In practice, such separation leads to inefficiencies in latency management, energy utilization, and adaptive routing, especially in robotic coordination systems.

Recent studies highlight that IoT communication protocols were initially designed for low-power sensor networks rather than dynamic robotic systems (Al-Sarawi et al., 2017; Sethi and Sarangi, 2017). Consequently, IoRT integration requires deeper cross-layer optimization where protocol decisions are shared across layers to enhance system efficiency.

Furthermore, the proliferation of heterogeneous communication standards such as Zigbee, Bluetooth Low Energy, LoRa, and IEEE 802.11ah introduces interoperability challenges in unified IoT–IoRT

ecosystems (Khorov et al., 2015; Want et al., 2013). These challenges are compounded by increasing security threats in IoT environments, including device-level vulnerabilities and network-layer exploitation (Bilal, 2017)

1.2 Problem Statement

Despite significant advancements in IoT architectures and robotic systems, there remains a lack of unified cross-layer protocol frameworks that effectively support IoT–IoRT convergence. Existing solutions are often siloed, focusing either on IoT communication efficiency or robotic autonomy, but rarely addressing their integration holistically. This leads to inefficiencies in data routing, increased latency in robotic decision loops, and vulnerability to security attacks (Bilal, 2017).

Additionally, conventional layered architectures restrict adaptive communication between network layers, limiting optimization opportunities for energy consumption, reliability, and real-time performance. The absence of standardized cross-layer coordination mechanisms further exacerbates interoperability issues among heterogeneous devices and protocols.

1.3 Research Objectives

This paper aims to:

1. Analyze existing IoT and IoRT communication architectures and protocols.
2. Examine cross-layer design principles applicable to integrated systems.
3. Identify challenges in interoperability, scalability, and security.
4. Evaluate enabling technologies for IoT–IoRT convergence.
5. Propose conceptual insights for future cross-layer protocol optimization.

1.4 Scope and Significance

The scope of this study is limited to protocol-level and architectural analysis of IoT–IoRT systems. It does not focus on hardware design or application-specific robotics but rather emphasizes communication strategies and system-level integration. The significance of this research lies in its potential to guide the development of next-generation intelligent infrastructures capable of supporting autonomous robotics within IoT ecosystems.

2. Literature Review

2.1 Evolution of IoT Architectures

The foundational framework of IoT was introduced by Atzori et al. (2010), who defined IoT as a paradigm integrating uniquely identifiable objects with Internet connectivity. Their survey highlighted three major architectural visions: semantic-oriented, service-oriented, and network-oriented IoT. This work established the conceptual basis for later architectural expansions.

Gubbi et al. (2013) extended this model by introducing a cloud-centric IoT architecture comprising sensing, network, data management, and application layers. Their study emphasized scalability and cloud integration, laying groundwork for distributed IoT systems.

However, both studies primarily assume static sensing environments and do not account for robotic mobility or real-time actuation constraints required in IoRT systems.

2.2 IoT Communication Protocols and Standards

A significant body of literature focuses on IoT protocol stacks and communication technologies. Al-Sarawi et al. (2017) provide a comprehensive review of IoT communication protocols, including MQTT, CoAP, Zigbee, and 6LoWPAN, highlighting their suitability for constrained environments. Similarly, Sethi and Sarangi (2017) analyze IoT architectures and protocols, emphasizing layered communication models and interoperability challenges.

Salman and Jain (2017) further categorize IoT protocols based on application requirements, particularly addressing scalability and latency trade-offs. These works collectively demonstrate that IoT protocol design prioritizes energy efficiency and low bandwidth usage.

However, these protocols are not inherently designed for robotic systems requiring deterministic latency and real-time responsiveness.

2.3 IoRT and Robotic Communication Systems

The concept of IoRT, introduced by Ray (2017), expands IoT capabilities by integrating intelligent robotic systems capable of sensing, computation, and autonomous action. IoRT systems rely on continuous feedback loops and require ultra-low latency communication channels for real-time decision-making.

Ray (2017) emphasizes challenges such as distributed intelligence, secure communication, and coordination among robotic agents. These requirements significantly exceed the capabilities of traditional IoT protocols, highlighting the need for cross-layer optimization.

2.4 Low-Power and Short-Range Communication Technologies

Several studies focus on underlying communication technologies supporting IoT systems. IEEE 802.11ah has been identified as a key enabler for smart city

deployments due to its extended range and low power consumption (Khorov et al., 2015). Similarly, Bluetooth Low Energy has gained popularity for short-range IoT communication due to its energy efficiency (Want et al., 2013).

LoRa technology provides long-range communication for low-power devices, making it suitable for distributed IoT networks (Aloÿs et al., 2016). However, these technologies are often isolated in deployment scenarios and lack unified interoperability frameworks.

2.5 Embedded Systems and Serial Communication Protocols

IoT and IoRT systems rely heavily on embedded communication protocols such as SPI, UART, and I2C for device-level integration. These protocols enable low-level data exchange between sensors, actuators, and microcontrollers (Renesas Application Note, 2003; Valdez and Becker, 2015).

Murphy (2011) and Grusin (2010) highlight USB and SPI as fundamental communication standards for embedded IoT systems. While efficient for device-level communication, they do not scale effectively for network-wide IoT–IoRT integration.

2.6 Security and Vulnerability Concerns

Security remains a critical challenge in IoT ecosystems. Bilal (2017) provides an in-depth analysis of IoT architecture vulnerabilities, highlighting risks such as unauthorized access, data interception, and device manipulation, particularly in smart manufacturing systems such as 3D printing environments. This underscores the necessity of integrating security considerations at all protocol layers rather than treating them as an isolated concern.

2.7 Research Gaps

The literature reveals several unresolved issues:

- Lack of unified cross-layer protocol frameworks for IoT–IoRT integration
- Limited support for real-time robotic communication in IoT protocols
- Fragmented interoperability across heterogeneous communication standards
- Insufficient integration of security into cross-layer design
- Absence of adaptive routing mechanisms supporting robotic mobility

These gaps necessitate a holistic cross-layer protocol design approach capable of bridging IoT sensing networks with IoRT autonomous systems.

3. Methodology

3.1 Research Design

This study adopts a qualitative analytical review methodology based on systematic synthesis of existing IoT and IoRT literature. The approach focuses on comparative analysis of architectural models, protocol stacks, and communication frameworks to identify integration challenges and optimization opportunities.

The analysis framework is structured around three core dimensions:

1. Architectural Layer Analysis – examining interaction between physical, network, transport, and application layers.

2. Protocol Efficiency Assessment – evaluating performance characteristics such as latency, scalability, and energy consumption.

3. Cross-Layer Integration Feasibility – assessing adaptability of protocols in IoT–IoRT hybrid systems.

3.2 Analytical Framework Overview

The study conceptualizes IoT–IoRT systems as multi-layered adaptive networks where cross-layer communication enables dynamic optimization. Unlike traditional static models, cross-layer design allows feedback exchange between layers to improve routing efficiency, reduce latency, and enhance system reliability.

Bilal (2017) is referenced in evaluating how security vulnerabilities propagate across layers in IoT architectures, reinforcing the need for integrated defense mechanisms embedded within protocol design.

3.3 Cross-Layer Protocol Design Perspective

Cross-layer design in IoT–IoRT systems departs from the traditional OSI model by enabling interaction between non-adjacent layers to optimize system performance. Instead of treating each layer independently, cross-layer approaches allow shared information exchange between sensing, routing, MAC, transport, and application layers.

In IoT environments, this is particularly relevant for optimizing energy consumption and throughput in constrained devices. However, in IoRT systems, the requirement extends further to include deterministic latency, motion coordination, and real-time feedback control loops (Ray, 2017). This necessitates a unified protocol adaptation mechanism where network conditions directly influence robotic decision-making.

Bilal (2017) highlights that isolated layer designs increase vulnerability exposure, as attackers can exploit

inconsistencies between layers. Therefore, cross-layer security integration becomes essential, ensuring that authentication, encryption, and anomaly detection mechanisms operate cohesively across the stack.

3.4 IoT–IoRT Integration Architecture Model

The proposed analytical model is structured into four integrated layers:

(i) Perception Layer

This layer consists of sensors, actuators, and robotic perception modules. It collects environmental data and converts it into digital signals. In IoRT, this layer includes cameras, LiDAR, and robotic motion sensors.

(ii) Communication Layer

Responsible for data transmission using heterogeneous protocols such as Zigbee, BLE, LoRa, IEEE 802.11ah, and Ethernet-based systems. Protocol selection depends on range, latency, and energy constraints (Khorov et al., 2015; Aloÿs et al., 2016).

(iii) Cross-Layer Optimization Layer

This is the core analytical layer where protocol decisions are dynamically adjusted. It integrates routing efficiency, congestion control, and energy optimization strategies. Unlike traditional models, this layer continuously interacts with both perception and application layers.

(iv) Application & Control Layer

This layer executes decision-making algorithms, robotic control commands, and IoT service logic. In IoRT systems, this includes autonomous navigation, industrial automation, and smart surveillance applications (Ray, 2017).

3.5 Data Synthesis Approach

The methodology relies on structured comparative synthesis of literature rather than empirical experimentation. Each reference is analyzed based on:

- Protocol characteristics
- Architectural contribution
- Layer interaction model
- Suitability for IoT vs IoRT environments
- Security and scalability considerations

This comparative framework enables identification of convergence points and mismatches between IoT and IoRT systems.

4. Results / Findings

The analysis reveals that existing IoT communication architectures are fundamentally optimized for low-power, static, and delay-tolerant environments, whereas IoRT systems demand high adaptability, deterministic latency, and continuous feedback loops. This mismatch creates significant inefficiencies when both paradigms are integrated without cross-layer optimization mechanisms.

First, IoT protocols such as MQTT, CoAP, and Zigbee demonstrate strong energy efficiency but lack real-time guarantees required for robotic coordination. For instance, lightweight publish-subscribe models are effective for sensor data aggregation but introduce unpredictable latency under high network congestion. In contrast, IoRT systems require synchronized communication between robotic agents, which cannot tolerate such variability (Ray, 2017).

Second, the study finds that heterogeneous communication technologies (BLE, LoRa, IEEE 802.11ah) operate in isolated performance domains, leading to fragmentation in IoT–IoRT environments. While LoRa excels in long-range communication with minimal energy consumption (Aloÿs et al., 2016), it is unsuitable for high-frequency robotic control signals. Conversely, BLE provides short-range efficiency but fails to scale in distributed robotic networks.

Third, embedded communication protocols such as SPI, UART, and I2C are essential for intra-device communication but do not contribute directly to network-level interoperability. Their role is confined to sensor-actuator coordination within individual robotic units, limiting their scalability in IoT ecosystems (Renesas Application Note, 2003; Valdez and Becker, 2015).

Fourth, security vulnerabilities remain a critical concern. Bilal (2017) demonstrates that IoT systems, particularly in industrial environments such as 3D printing networks, are highly susceptible to multi-layer attacks. The findings suggest that lack of cross-layer security integration allows attackers to exploit inconsistencies between application-level authentication and network-level transmission protocols.

Fifth, IEEE 802.11ah and similar low-power wide-area technologies show promise in bridging IoT and IoRT systems due to their extended range and moderate energy efficiency (Khorov et al., 2015). However, their latency performance is still insufficient for real-time robotic coordination tasks.

Overall, the results indicate that no single protocol or communication standard is capable of supporting full IoT–IoRT convergence. Instead, a hybrid cross-layer optimization framework is required to dynamically adapt protocol behavior based on context, device state, and application requirements. This reinforces the need for integrated architectures that combine adaptive

routing, energy-aware scheduling, and real-time prioritization mechanisms.

5. Discussion

The findings of this study highlight a fundamental architectural conflict between IoT and IoRT systems. IoT networks prioritize scalability, energy efficiency, and intermittent communication, while IoRT systems demand continuous, deterministic, and low-latency interactions. This divergence necessitates a paradigm shift from traditional layered models toward cross-layer protocol design.

From a theoretical perspective, the study aligns with Gubbi et al. (2013), who emphasized layered IoT architectures but did not fully account for robotic actuation requirements. Similarly, Atzori et al. (2010) provided foundational IoT classifications but lacked integration with autonomous robotic control systems. The current analysis extends these models by introducing cross-layer interaction as a bridging mechanism.

Practically, cross-layer design enables adaptive decision-making where lower-layer network conditions influence higher-layer application behavior. For example, robotic path planning systems can adjust movement trajectories based on network congestion or latency variations. This dynamic adaptation is essential for industrial IoRT deployments such as automated warehouses and smart manufacturing systems.

However, implementing cross-layer protocols introduces significant trade-offs. Increased inter-layer dependency can lead to system complexity and reduced modularity. Additionally, real-time synchronization across layers may introduce computational overhead, particularly in resource-constrained devices. These challenges highlight the need for lightweight cross-layer optimization algorithms.

Security implications are also critical. As demonstrated by Bilal (2017), vulnerabilities in IoT systems often arise due to inconsistent security enforcement across protocol layers. Cross-layer integration must therefore incorporate unified security policies, ensuring consistent authentication and encryption across all communication stages.

Another key limitation is interoperability. While technologies such as BLE, LoRa, and IEEE 802.11ah provide diverse connectivity options (Want et al., 2013; Aloÿs et al., 2016), their lack of standardized cross-layer coordination limits seamless integration. This fragmentation reduces system reliability in heterogeneous environments.

Despite these challenges, cross-layer design offers substantial benefits. It enables improved resource utilization, reduced communication latency, and enhanced adaptability in dynamic environments. In IoRT systems, this translates into more efficient robotic coordination, improved autonomy, and higher operational resilience.

Ultimately, the study demonstrates that IoT–IoRT convergence cannot be achieved through incremental improvements in existing protocols. Instead, it requires a rethinking of protocol architecture itself, shifting from rigid layered models to adaptive, context-aware cross-layer frameworks.

6. Conclusion

This paper presented a comprehensive analytical review of cross-layer protocol design and integration strategies for IoT and IoRT convergence. The study examined existing communication architectures, protocol standards, and embedded systems to identify limitations in supporting integrated intelligent environments.

The findings confirm that traditional IoT protocols are insufficient for IoRT applications due to their inability to support real-time, deterministic, and high-mobility communication requirements. IoRT systems introduce additional complexity through autonomous robotic behavior, requiring continuous feedback loops and adaptive coordination mechanisms (Ray, 2017).

The study highlights that heterogeneity in communication technologies—ranging from BLE and LoRa to IEEE 802.11ah—creates fragmentation in IoT–IoRT ecosystems. While these technologies individually provide optimized solutions for specific use cases, they lack interoperability at the cross-layer level (Khorov et al., 2015; Aloÿs et al., 2016).

A major contribution of this work is the identification of cross-layer optimization as a critical enabler for IoT–IoRT integration. By allowing interaction between protocol layers, systems can dynamically adapt to changing network conditions, optimize energy usage, and improve real-time responsiveness.

Security remains a persistent challenge, as highlighted by Bilal (2017), where multi-layer vulnerabilities necessitate integrated defense mechanisms across protocol stacks. Future systems must embed security directly into cross-layer design rather than treating it as an external component.

Future research should focus on developing lightweight cross-layer algorithms, standardized interoperability frameworks, and AI-driven adaptive routing mechanisms. Additionally, experimental validation of proposed models in real-world IoRT environments such as industrial automation and smart logistics is essential.

In conclusion, cross-layer protocol design represents a foundational approach for achieving seamless IoT–IoRT convergence, enabling the next generation of intelligent, autonomous, and interconnected systems.

References

1. Abdmeziem, M. R., Tandjaoui, D., and Romdhani, I. (2015). Architecture of the The Internet of things: State of the Art. Springer, 9
2. Aloÿs, A., JiaziYi , T. C.& William, M. T. (2016). A Study of LoRa: Long Range & Low Power Networks for the The Internet of things
3. Al-Sarawi, S., Anbar, M., Alieyan, K., Alzubaidi, M. (2017). The Internet of things (IoT) Communication Protocols:Review. 8th International Conference on Information Technology (ICIT), 685-690.
4. Atzori L., Iera,A.,Morabito G. (2010). The theInternet of things: a survey. Elsevier Computer networks,54: 2787–2805.
5. Bilal, M. (2017). A Review of The Internet of things Architecture, Technologies and Analysis Smartphone-based Attacks Against 3D printers, Elsevier, 4.
6. Colin M. L. B. (2006). A single master and a single slave on a Serial Peripheral Interface (SPI) bus, Free Software FoundationCypress(2014). An Introduction to Universal Serial Bus 2.0.
7. Cypress (2014). An Introduction to Universal Serial Bus 2.0.
8. DesignSpark (2012).
9. Evans, D. (2011). The The Internet of things: How the Next Evolution of the Internet is Changing Everything; San Jose, CA, USA, Cisco Internet Business Solutions Group.
10. Grusin M., 2010, Serial Peripheral Interface (SPI)
11. Gubbi, J.; Buyya, R.; Marusic, S.; Palaniswami, M. (2013). The Internet of things (IoT): A vision, architectural elements, and future directions. Future Gener. Comput. Syst., 1645–1660
12. Guibene, W., Nolan, K. E., Kelly, M. Y. (2015). Survey on clean slate cellular-IoT standard proposals. In Proceedings of the 2015 IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing (CIT/IUCC/DASC/PICOM), Liverpool, UK, 1596–1599.
13. IEEE 1394-The multimedia Bus of the Future, (2011)
14. ISO-IEC. ISO/IEC 18000-7. (2014). Information Technology—Radio Frequency Identification for Item Management—Part 7: Parameters for Active Air Interface Communications at 433 MHz; ISO: Geneva, Switherland.
15. Interoperable protocols of... Odirichukwu, J..C., Asagba, P.O., Onuodu F..E International Journal of Computing, Intelligence and Security Research 1(1)2021| 121
16. Khorov, E. Lyakhov, A. Krotov, A. Guschin, A. (2015). A survey on ieee 802.11 ah: An enabling networking technology for smart cities. Comput. Commun.58, 53–69.
17. Laddha, N. R., and Thakare, A. P. (2013). Implementation of Serial Communication using UART with Configurable Baud Rate. International Journal on Recent and Innovation Trends in Computing and Communication, 1(4): 263-268.
18. Margelis, G., Piechocki, R. Kaleshi, D. Thomas, P. (2015). Low throughput networks for the IoT: Lessons learned from industrial implementations. In Proceedings of the 2015 IEEE 2nd World Forum on The Internet of things (WF-IoT), Milan, Italy, 14–16.
19. Meritt, C. (2016). SPI peripheral use case example
20. Murphy, R. (2011). An Introduction to universal Serial Bus 2.0
21. Pervasive computing, (2016).
22. Patel, K. K., and Patel, S. M. (2016). The Internet of things IOT: Definition, Characteristics, Architecture, Enabling Technologies, Application & Future Challenges. International Journal of Engineering Science and Computing, 6(5):6122.
23. Rajiv. (2018). Applications of Z-wave technology.
24. Ray, P. P. (2017). Internet of Robotic Things: Concept, Technologies, and Challenges, IEEE Access, 4, 9489-9500.
25. Renesas Application Note. (2003). SPI. AN0303011/Rev1.00, 1-14
26. Salman, T., Jain, R. (2017). A Survey of Protocols and Standards for Internet of Things. Advanced Computing and Communications, 1(1):1-20.
27. Sethi, P., and Sarangi, S. R. (2017). The Internet of things: Architectures, Protocols, and Applications. Journal of Electrical and Computer Engineering, 25.
28. Shetye, T. (2018). Universal Synchronous Asynchronous Receiver Transmitter (USART).

29. Shiba, K.V. (2009). Introduction to Embedded Systems, New Delhi, Tata McGraw Hill Education Private Limited, 45-49.

30. SIGMA DESIGN. (2014). Z-Wave wireless Communications for Smart Devices and IoT, Z-Wave Technical Working Group

31. UART . (2016). Serial communication.

32. Valdez, J., Becker, J. (2015). Understanding the I2C Bus, Texas Instrument, 1-6

33. Want, R., Schilit, B., Laskowski, D. (2013). Bluetooth le finds its niche. IEEE Pervasive Comput.12, 12–16.