International Journal of Electrical and Computer Engineering (IJECE)
Vol. 16, No. 3, June 2026, pp. 1626∼1644
ISSN: 2088-8708, DOI: 10.11591/ijece.v16i3.pp1626-1644

AMAC-LW: Adaptive medium access control for long range wide area network with energy-aware routing

Sowmya M.[1], S. Meenakshi Sundaram[2], Pandiyanathan Murugesan[3], Santhosh Kumar K. S.[4], Tejaswini R. Murgod[5]
[1]Department of Artificial Intelligence and Data Science, Nitte Meenakshi Institute of Technology, Bengaluru, India
[2]Department of Computer Science and Engineering, ACS College of Engineering, Bengaluru, India
[3]Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, India
[4]Department of Artificial Intelligence and Machine Learning, Mysore University School of Engineering, University of Mysore, Mysuru, India
[5]Department of Artificial Intelligence and Machine Learning, B N M Institute of Technology, Bengaluru, India

Article Info

Article history:

Received Dec 14, 2024
Revised Jan 21, 2026
Accepted Mar 16, 2026

Keywords:

Data communication efficiency
Energy-efficient
LoRaWAN networks
MAC layer
Optimized routing algorithm
Packet delivery ratio
Security

ABSTRACT

To enhance the performance of long range wide area network (LoRaWAN), a routing algorithm and a novel medium access control (MAC) layer protocol are required. In addition to addressing scalability and security issues, the protocol seeks to improve communication efficiency, dependability, and power consumption. It presents a dynamic routing method that reduces energy consumption by utilizing machine learning processes, adaptive routing tactics, and route optimization approaches. Simulations in a range of deployment situations are used to assess the suggested solutions. These results imply that the suggested protocol and routing scheme have the potential to greatly enhance the sustainability, energy efficiency, and performance of LoRaWAN-based Internet of Things networks. The effectiveness of the proposed solutions is evaluated through extensive simulations across diverse deployment scenarios. The results demonstrate that the proposed MAC protocol achieves a throughput of 350 bps, outperforming conventional protocols that typically reach only 220 bps. Latency is reduced to 50 ms from 85 ms, energy consumption is decreased to 2.5 joules from 4.5 joules, and the packet delivery ratio (PDR) is improved to 95%, compared to 75% in existing approaches. These findings highlight the potential of the proposed protocol and routing scheme to significantly enhance the performance, energy efficiency, and sustainability of LoRaWAN-based IoT networks.

Corresponding Author:

Sowmya M.
Department of Artificial Intelligence & Data Science, Nitte Meenakshi Institute of Technology
Bengaluru-560064, India
Email: sanu.196@gmail.com

1. INTRODUCTION

The Internet of Things (IoT) is revolutionizing digital and physical environments, leading to vast interconnected networks of sensors, devices, and smart systems. Low power wide area networks (LPWANs) have become crucial for IoT deployments due to their long-range connectivity and low energy consumption. Long range wide area network (LoRaWAN) a widely adopted LPWAN protocol, is scalable, flexible, and cost-effective, making it suitable for low-power, battery-operated devices. However, to fully realize the potential of LoRaWAN in large-scale IoT ecosystems, performance-related challenges at both the medium access control (MAC) and routing layers need to be addressed. LPWAN technologies enable IoT devices to communicate over long distances with minimal power consumption, and LoRaWAN has gained widespread adoption due to its flexible architecture, low deployment cost, and suitability for low-data-rate, long-range communication scenarios. This study aims to address the need for reliable and energy-efficient communication in IoT deployments. Standard LoRaWAN protocols, while adequate for basic operations, struggle in dynamic environments with high node density, frequent data transmission, and intelligent decision-making. IoT applications in smart cities, healthcare, and industrial automation require protocols that can adapt in real-time, consume minimal energy, and maintain secure data delivery. Existing MAC protocols in LoRaWAN lack adaptability and intelligence, prompting the development of enhanced solutions. Machine learning-based techniques are integrated into routing and scheduling mechanisms to ensure data integrity and minimize energy consumption. LoRaWAN operates on the LoRa modulation technique, which uses chirp spread spectrum (CSS) for long-range communication. However, traditional advocates of linux open-source hawaii association (ALOHA)-based access schemes result in increased collision probability, packet loss, and energy inefficiencies. Researchers are exploring more advanced MAC and routing protocols for performance enhancement and energy optimization.

LoRaWAN is a versatile IoT communication protocol that offers long-range communication, low power consumption, scalability, and cost-effectiveness. It supports thousands of end devices per gateway and is energy-efficient, allowing devices to spend most of their time in low-power sleep modes. LoRaWAN also supports bidirectional communication, enabling data transmission and remote control. It also supports mobility to some extent. However, LoRaWAN has limitations, such as a lower data rate compared to other wireless technologies, increased network congestion and packet collisions in dense deployments, and limited quality of service (QoS) due to its reliance on the ALOHA protocol. Basic implementations may also lack advanced intrusion detection or anomaly mitigation mechanisms. These trade-offs highlight the need for continued optimization in LoRaWAN protocol design to meet the evolving demands of IoT systems. LoRaWAN is a wireless communication system that consists of three classes of end devices are class A, class B, and class C. Class A is the most energy-efficient mode, ensuring minimal energy usage for battery-powered sensors used in agriculture or utility metering. Class B synchronizes devices with beacons from the gateway, allowing for predictable downlink communication. Class C, the most responsive class, keeps the device's receiver open except during transmission, providing the lowest latency for downlink messages. Each class caters to different IoT use cases, with class A for ultra-low power needs, class B for balanced control and power, and class C for latency-critical operations. However, the performance of LoRaWAN in demanding applications can be significantly improved through the integration of intelligent MAC layer protocols and energy-aware routing strategies. These enhancements are essential for scaling LoRaWAN to meet the requirements of next-generation IoT networks.

As depicted in Figure 1, the adaptive MAC protocol for LoRaWAN (AMAC-LW) is structured in a layered and modular fashion, enabling intelligent coordination of communication processes within IoT networks. At the top, the application layer interfaces directly with the AMAC-LW protocol, which serves as the central medium access control entity responsible for managing transmission requests, acknowledgments, and communication orchestration between end-devices and gateways. The AMAC-LW protocol is composed of three core components: the MAC common part sublayer (MCPS), which facilitates data transmission and reception; the MAC layer management entity (MLME), which oversees essential network management tasks such as joining procedures and scheduling; and the MAC information base (MIB), which stores runtime configurations and operational state data required for protocol execution. In addition to these primary elements, AMAC-LW incorporates several adaptive enhancements that further optimize performance. Dynamic duty cycling adjusts device activity periods in response to traffic load and energy conditions, while congestion-aware routing selects optimal paths to alleviate network bottlenecks. Energy efficiency optimization mechanisms are embedded to prolong battery life without sacrificing reliability. Security is reinforced through integrated encryption, authentication, and anomaly detection techniques. Scalability is addressed through dynamic parameter tuning, enabling seamless network expansion. Moreover, the protocol benefits from machine learning enhancements that leverage historical patterns to inform smarter decisions in both routing and MAC operations. Collectively, these features enable AMAC-LW to deliver high-performance, energy-efficient, and scalable communication suitable for modern IoT environments.

The existing medium access control (MAC) protocols in LoRaWAN face significant limitations when deployed in dense or large-scale networks. The basic LoRaWAN MAC layer, which follows a pure ALOHA scheme, suffers from high packet collision rates, lacks efficient scheduling and resource allocation strategies, resulting in suboptimal throughput, increased latency, excessive energy consumption, and challenges in maintaining scalability and security. To address these shortcomings, an enhanced MAC protocol architecture, called AMAC-LW, is introduced. This protocol integrates adaptive communication mechanisms and intelligent decision-making capabilities, ensuring reliable, energy-efficient, and secure data transmission across IoT networks. Energy-efficient routing is also crucial in LoRaWAN, as traditional mechanisms often ignore dynamic changes in network topology and node energy status, leading to uneven energy depletion, bottlenecks, and reduced network lifetime. An energy-efficient and congestion-aware routing algorithm is proposed to ensure sustained performance and balanced energy usage across the network.

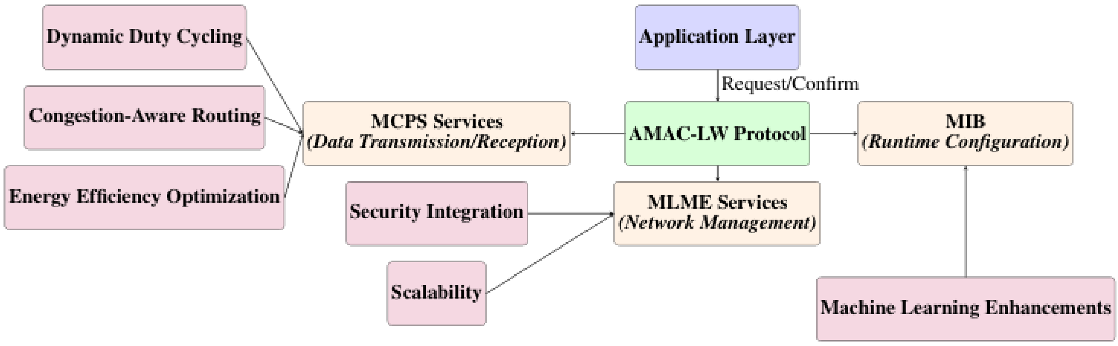


Figure 1. Adaptive MAC protocol for LoRaWAN (AMAC-LW) architecture

2. RELATED WORK

Li *et al.* [1] proposed the CGBS-LoRa MAC protocol, which significantly improves the scalability of LoRa networks and reduces device collisions. The protocol maintains a high packet delivery rate and low latency, even as the LoRaWAN network grows. Chasserat *et al.* [2] introduced LoRaSync, a time-slotted ALOHA-based access method that uses a clock drift model from real low-cost devices. Their solution enhances throughput and energy efficiency, with performance validated through simulations and testbed implementation. Paul *et al.* [3] developed a framework to assist LoRaWAN network designers in selecting or creating models tailored to specific application requirements such as delay and device lifetime. The framework incorporates simulation-based comparisons of single-hop and multi-hop routing. Jouhari *et al.* [4] conducted a comprehensive survey of LoRaWAN scalability issues at the physical and MAC layers, focusing on capacity expansion and interference reduction. The study highlights existing solutions such as spreading factor optimization, channel assignment, and alternative topologies. Chen *et al.* [5] modeled class-A LoRaWAN devices using probabilistic timed automata (PTA) to capture timing behavior, transmission schedules, and collision dynamics. They used the PRISM model checker for quantitative analysis under various conditions. Leonardi *et al.* [6] also employed PTA and PRISM to model and analyze class-A LoRaWAN behavior, emphasizing MAC layer interactions and performance evaluation under different network scenarios.

Ahmar *et al.* [7] proposed a time-synchronized cryptographic frequency hopping MAC protocol that enhances LoRa's scalability, security, and reliability. The protocol demonstrates superior performance and resistance to selective jamming compared to conventional LoRaWAN. Chen *et al.* [8] analyzed denial-of-service (DoS) vulnerabilities in LoRaWAN's MAC layer and proposed two targeted attacks on confirmed transmissions. Their findings show that even a small number of attackers can significantly reduce packet success rates and energy efficiency. Li *et al.* [1] further emphasized improvements in ALOHA-based LoRaWAN communication through geographical segmentation and optimized transmission parameters, showing enhanced scalability and collision reduction in dense networks. Prasetyo *et al.* [9] proposed the LoRa multi-communication (LMC) protocol at the application layer. Designed for IoT devices with limited energy resources, the protocol improves battery life and packet reception based on experimental validation. Pirri *et al.* [10] proposed enabling LoRaWAN end-devices to support multiple MAC protocols to meet the quality of service (QoS) demands in industry 4.0 environments. Their method uses flow mapping to address various latency and reliability needs, while also highlighting several design challenges.

Chen *et al.* [11] investigated the impact of greedy behaviors by compromised nodes in LoRaWAN's MAC layer. They proposed a double judgment detection mechanism. Although LoRaWAN remains fairly resilient, extensive greedy behavior degrades performance. However, their approach effectively detects such activities. Leonardi *et al.* [12] conducted a simulation-based evaluation of the listen before talk adaptive frequency agility (LBT-AFA) MAC protocol for LoRaWAN under varying MAC parameters and node densities. Their findings guide MAC parameter optimization for improved latency and consistent performance. Dieng *et al.* [13] introduced a real-time, collision-free scheduling technique for LoRaWAN based on graph coloring. This method significantly enhances scalability and reliability for time-sensitive IoT applications, as evidenced by NS-3 simulation results showing reduced packet loss and improved deadline adherence. Li [14] proposed a hybrid access technique that combines S-ALOHA and TDMA to support both periodic and burst transmissions in LoRaWAN. MATLAB simulations demonstrated reduced collision rates and better channel utilization compared to standard LoRaWAN. Tsakmakis *et al.* [15] developed an adaptive hybrid MAC protocol based on learning automation. The protocol was shown through simulation to substantially reduce transmission latency when compared with conventional LoRaWAN approaches.

Cheikh *et al.* [16] provided a tutorial review of machine learning approaches for LoRaWAN resource optimization, including transmission power control and spreading factor tuning. They also identified accessible datasets, simulation tools, and outlined directions for ML-driven enhancements. Banti *et al.* [17] presented a comprehensive survey of LoRaWAN MAC protocols with a focus on energy efficiency. The study compares existing techniques, identifies limitations, and suggests future research directions. Alahmadi *et al.* [18] proposed the SBTS-LoRa MAC protocol, where nodes adjust transmission parameters based on their distance from the gateway. Simulation results showed significant improvements in throughput and scalability—up to 14×—compared to adaptive data rate (ADR) schemes. Xiao *et al.* [19] explored the integration of collision decoding techniques with MAC protocols in LoRa networks. They categorized and analyzed various decoding methods, examined their impact on MAC strategies, and proposed future research opportunities for massive IoT connectivity. Triantafyllou *et al.* [20] introduced TS-VP-LoRa, a time-slotted MAC scheme that incorporates gateway-coordinated scheduling and channel hopping to enhance LoRaWAN's scalability. Simulations demonstrated improvements in packet delivery, reduced latency, and fewer collisions, all while preserving energy efficiency in dense deployments. Zhong and Springer [21] proposed a time-slotted MAC protocol and edge-acknowledging architecture to improve reliability and energy efficiency in LoRaWAN confirmed messaging. Their approach enhances packet reception and energy savings, though it introduces additional delay in larger networks.

Chasserat *et al.* [22] presented TREMA, a traffic-aware and energy-efficient MAC protocol for LoRa. TREMA dynamically switches between synchronous and asynchronous communication to balance energy consumption and network capacity under varying traffic conditions. Farooq [23] developed a multi-hop routing protocol with a software-defined networking (SDN) extension for LoRa, aimed at achieving high data rates and extended coverage. Evaluations indicated a 5× increase in packet reception ratio and reduced energy consumption compared to traditional LoRa settings. Chinchilla-Romero *et al.* [24] proposed the CARA method, which uses efficient resource allocation, leveraging multi-channel access and spreading factor orthogonality. Both simulation and experimental results showed up to a 95.2% increase in LoRaWAN capacity and full compatibility with existing devices. Triantafyllou *et al.* [25] also proposed FCA-LoRa, a beacon-based MAC protocol designed to improve throughput in dense LoRaWAN networks. Simulations showed up to a 50% throughput improvement over enhanced ALOHA-based protocols. Garrido-Hidalgo *et al.* [26] implemented a practical low-overhead synchronization and scheduling system for class A LoRaWAN devices. Experimental results using SF12 achieved packet delivery ratios of up to 29%, validating its performance in high-load scenarios. Leonardi *et al.* [27] evaluated the performance impacts of updated ETSI regulation constraints on LoRaWAN MAC protocols, focusing on pure ALOHA and listen before talk (LBT). Their work provides simulation-based comparisons to assist with protocol selection under realistic traffic loads.

Table 1 presents a comparative analysis of several recent LoRaWAN MAC protocol enhancements based on selected works from the literature. These protocols aim to improve aspects such as throughput, energy efficiency, security, and scalability in IoT communication. For example, the work by Li *et al.* [1] introduces a grouped bit-slot approach to improve channel utilization, while Chasserat *et al.* [2] focus on energy-efficient synchronization through LoRaSync. Some studies, like that of Ahmar *et al.* [7], emphasize robust communication by handling packet collisions and ensuring fairness. Meanwhile, Chen *et al.* [8] and Jouhari *et al.* [4] analyze security concerns and DoS vulnerabilities in the MAC layer. Overall, the table shows that while most protocols enhance throughput and energy usage, only a few give detailed attention to security and large-scale deployment support.

This highlights the need for a comprehensive solution like AMAC-LW, which addresses all these aspects effectively. Table 2 presents recent MAC protocol developments tailored for LoRaWAN. These protocols vary from energy-efficient solutions like TREMA [22] and LoRaSync [2] to robust and secure models like the one proposed by Chen *et al.* [8]. Hybrid and planning-aware approaches [3, 6] enhance flexibility and network-wide optimization. Adaptive and event-triggered designs [1, 15] show promise in dynamic IoT environments.

Table 1. Comparison of selected LoRaWAN MAC protocols relevant to AMAC-LW

Work	Throughput	Energy Efficient	Security	Scalability
Li *et al.* [1]	✓	✓	✗	✓
Chasserat *et al.* [2]	✓	✓	✗	✓
Paul *et al.* [3]	✓	✓	✗	✓
Jouhari *et al.* [4]	✓	✓	✓	✓
Chen *et al.* [5]	✓	✗	✓	✓
Leonardi *et al.* [6]	✓	✓	✗	✓
Ahmar *et al.* [7]	✓	✓	✓	✓
Chen *et al.* [8]	✓	✗	✓	✗
Prasetyo *et al.* [9]	✓	✓	✗	✗
Pirri *et al.* [10]	✓	✓	✗	✓
Chen *et al.* [11]	✓	✗	✓	✓
Leonardi *et al.* [12]	✓	✓	✗	✓
Dieng *et al.* [13]	✓	✓	✗	✓
Li [14]	✓	✓	✗	✓
Tsakmakis *et al.* [15]	✓	✓	✗	✓
Cheikh *et al.* [16]	✓	✓	✗	✓
Banti *et al.* [17]	✓	✓	✗	✓
Alahmadi *et al.* [18]	✓	✓	✗	✓
Xiao *et al.* [19]	✓	✓	✗	✓
Triantafyllou *et al.* [20]	✓	✓	✗	✓
Zhong and Springer [21]	✓	✓	✓	✓
Chasserat *et al.* [22]	✓	✓	✗	✓
Farooq [23]	✓	✓	✗	✓
Chinchilla-Romero *et al.* [24]	✓	✓	✗	✓
Triantafyllou *et al.* [25]	✓	✓	✗	✓
Garrido-Hidalgo *et al.* [26]	✓	✓	✗	✓
Leonardi *et al.* [27]	✓	✓	✗	✓

Table 2. State-of-the-art MAC Protocols for LoRaWAN

Ref	MAC Protocol / Scheme	Focus Area	Strengths	Limitations
[1]	Circular Region Grouped Bit-Slot	Collision Reduction	Efficient channel use	No security support
[2]	LoRaSync	Synchronization	Energy-efficient sync	Sync overhead
[16]	Multi-layered MAC Energy Model	Energy Efficiency	Cross-layer optimized	Integration complexity
[22]	TREMA	Traffic Awareness	Energy-efficient load	Complex coordination
[8]	Secure DoS-resilient MAC	Security	Jamming defense	Crypto overhead
[3]	LoRaWAN Planning-Aware MAC	Network Optimization	Improved coverage/QoS	Static assumptions
[9]	Novel MAC for Non-LoRaWAN	Alternative Framework	Independence	Compatibility limits
[6]	Combined MAC Schemes	Hybrid Design	Versatile operations	Coordination overhead
[15]	Adaptive MAC for Event Detection	Event-Driven Access	Reduced latency	Hardware dependency
[21]	Confirmed Traffic-Aware MAC	Reliability	Enhanced ACK handling	Confirmation overhead

3. PROBLEM STATEMENT

The current MAC protocols in LoRaWAN have limitations in data communication efficiency, reliability, energy consumption, security, and scalability. A comprehensive analysis of these protocols is needed to develop a new protocol tailored to specific IoT applications. Energy-efficient routing algorithms are crucial for minimizing energy consumption in LoRaWAN networks, impacting device longevity and network performance. Challenges include maintaining device security while reducing energy usage, managing network congestion, and adapting to dynamic network conditions. Innovative solutions incorporating machine learning and artificial intelligence techniques, dynamic routing adaptations, and hybrid approaches are needed to enhance the performance of routing algorithms and ensure energy efficiency and security within LoRaWAN environments.

4. PROPOSED SOLUTION

Addressing the challenges identified in the MAC layer protocols and routing algorithms in LoRaWAN includes the following stages.

4.1. Proposed model: adaptive MAC protocol for LoRaWAN (AMAC-LW) model

The adaptive MAC protocol for LoRaWAN (AMAC-LW) is designed to address the key challenges of data communication in LoRaWAN networks is as shown in Figure 2, focusing on optimizing efficiency, reliability, energy consumption, security, and scalability. Below are the main features and functionalities of the proposed model:

a. Dynamic duty cycling: The protocol implements adaptive duty cycling strategies that allow nodes to adjust their active and sleep periods based on real-time traffic conditions. This optimizes energy consumption by ensuring that nodes are awake only when data needs to be transmitted or received, extending battery life.
b. Congestion-aware routing: AMAC-LW integrates a congestion-aware routing mechanism that continuously monitors network traffic and identifies congested paths. When congestion is detected, the protocol reroutes data through alternative paths, reducing the likelihood of packet loss and enhancing overall network performance.
c. Energy efficiency optimization: The model employs energy-efficient routing algorithms that minimize the distance data must travel and the number of hops required. By optimizing these factors, the protocol reduces energy consumption, which is crucial for battery-operated IoT devices.
d. Security integration: security measures are seamlessly integrated into the protocol without significantly affecting energy consumption. The model employs lightweight encryption methods to ensure data confidentiality and integrity during transmission, addressing concerns over data privacy in LoRaWAN networks.

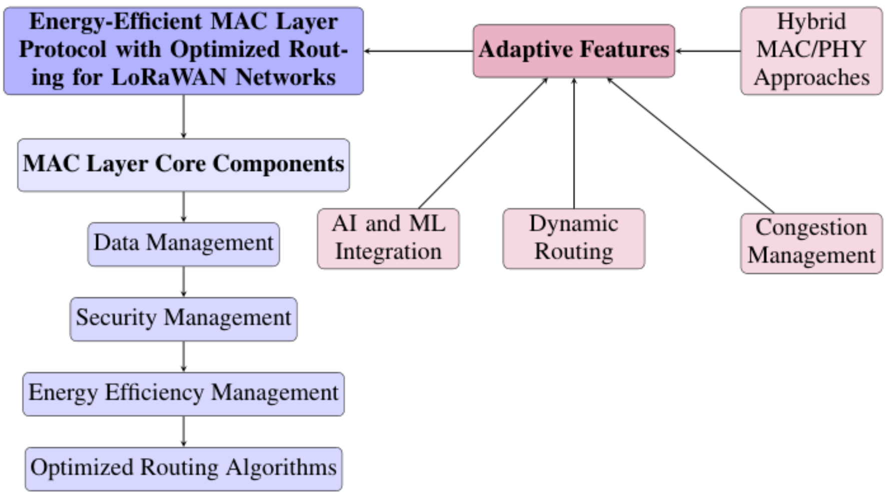


Figure 2. Proposed model for energy-efficient MAC layer protocol with optimized routing in LoRaWAN

Table 3 outlines the integration of multiple security mechanisms within the proposed AMAC-LW framework. At the physical (PHY) and MAC layers, AES-128 or AES-256 encryption ensures data confidentiality during transmission using MCPS services. Authentication is enforced using a message integrity code (MIC), particularly during the join procedure, leveraging MLME services to ensure message authenticity and prevent spoofing attacks. Key management is handled dynamically through the NwkSKey and AppSKey, which are managed via MIB configurations and MLME runtime services. Replay protection is achieved by verifying frame counters within the MLME layer, safeguarding against message duplication and delay attacks. Additionally, adaptive security is integrated through machine learning models that detect anomalies in traffic patterns—such as abnormal message frequency or structure—allowing the system to adaptively respond to emerging threats. This layered and integrated approach provides a robust foundation for ensuring both security and energy efficiency in LoRaWAN-based IoT applications.

a. Scalability: the proposed model is designed to be scalable, allowing it to adapt to varying network sizes and densities. It can efficiently manage large numbers of nodes and different communication patterns, making it suitable for diverse IoT applications.
b. Machine learning enhancements: AMAC-LW incorporates machine learning techniques to improve routing decisions based on historical and real-time data. This allows the protocol to learn and adapt to changing network conditions, enhancing its performance over time.
c. Simulation-based evaluation: The model will be evaluated through simulations that replicate various deployment scenarios, assessing its performance in terms of throughput, latency, energy consumption, and reliability against existing protocols.

Table 3. Security integration in AMAC-LW: adaptive medium access control for LoRaWAN

Security Layer	Technique	Integration Point
Encryption	AES-256	Applied at PHY and MAC payload levels through MCPS Services
Authentication	MIC (Message Integrity Code)	Enforced through Join Request/Accept via MLME Services
Key Management	NwkSKey and AppSKey	Managed via MIB runtime and supported by MLME layer
Replay Protection	Frame counter verification	Implemented within MLME Services to prevent duplication
Adaptive Security	Machine Learning detection	Integrated through MLME and Security Integration module

The AMAC-LW model represents a comprehensive approach to enhancing LoRaWAN data communication by focusing on energy efficiency, dynamic adaptability, and robust security features. By addressing the limitations of existing MAC protocols and incorporating innovative routing strategies, the model aims to improve the overall effectiveness and reliability of IoT applications in LoRaWAN networks.

4.2. Proposed method: implementation of the adaptive MAC protocol for LoRaWAN (AMAC-LW)

This proposed protocol integrates energy-efficient routing, dynamic network adaptations, and AI-driven security, with emphasis on IoT device longevity and efficient data communication within LoRaWAN networks.

a. Conduct a thorough literature review of existing MAC protocols in LoRaWAN to identify their strengths and limitations. This analysis helps to inform the design of the AMAC-LW by highlighting areas for improvement, such as energy consumption, reliability, and scalability.
b. The proposed method for developing the AMAC-LW involves a structured approach that begins with thorough analysis and design, followed by algorithm development, simulation testing, and iterative refinement.
c. By focusing on the unique needs of IoT applications and leveraging advanced routing and energy-efficient strategies, the AMAC-LW aims to enhance the effectiveness of data communication in LoRaWAN networks significantly.

4.3. Mathematical model

The proposed adaptive medium access control for long range wide area network (AMAC-LW) defines various parameters, variables, and equations representing the core components of the protocol. The model captures duty cycling, routing algorithms, energy consumption, and performance metrics.

4.3.1. Key parameters and variables

- N: Total number of nodes in the network
- D_i: Data rate of node i (bits/second)
- L: Average packet size (bits)
- R: Transmission range of each node (meters)
- T_{active}: Time a node remains active (seconds)
- T_{idle}: Time a node remains idle (seconds)
- P_{trans}: Power consumed during transmission (watts)
- P_{recv}: Power consumed during reception (watts)
- P_{idle}: Power consumed during idle state (watts)
- E_{total}: Total energy consumed by a node (joules)
- E_{battery}: Battery energy capacity of a node (joules)

– T_{latency}: End-to-end latency (seconds)
– $T_{\text{throughput}}$: Network throughput (bits/second)
– C: Channel capacity (bits/second)
– P_{success}: Probability of successful packet delivery
– C_{cong}: Network congestion metric

The AMAC-LW protocol incorporates energy-aware and traffic-adaptive mechanisms for efficient MAC scheduling. The mathematical model below details energy consumption, latency, reliability, and adaptive behaviors.

4.4. Duty cycling

Duty cycling reduces idle listening and overall energy consumption:

$$DC_i = \frac{T^i_{\text{active}}}{T^i_{\text{active}} + T^i_{\text{idle}}} \tag{1}$$

The node adapts its duty cycle based on the local traffic load:

$$T^i_{\text{active}} = T_{\min} + \kappa \cdot \text{Load}_i \tag{2}$$

where $T_{\min}$ is a minimum active duration, κ is a tunable coefficient, and Load_i is a number of packets in the buffer of node i.

4.5. Energy consumption model

a. Per-state energy

$$E_{\text{trans}} = P_{\text{trans}} \cdot T_{\text{trans}} \tag{3}$$
$$E_{\text{recv}} = P_{\text{recv}} \cdot T_{\text{recv}} \tag{4}$$
$$E_{\text{idle}} = P_{\text{idle}} \cdot T_{\text{idle}} \tag{5}$$

b. Total energy

$$E^i_{\text{total}} = E^i_{\text{trans}} + E^i_{\text{recv}} + E^i_{\text{idle}} \tag{6}$$

c. Energy per bit

$$E_{\text{bit}} = \frac{E_{\text{total}}}{L} \tag{7}$$

d. Energy efficiency

$$\eta_E = \frac{L \cdot P_{\text{success}}}{E_{\text{total}}} \tag{8}$$

4.6. Latency and delay model

$$T_{\text{latency}} = T_{\text{queue}} + T_{\text{access}} + T_{\text{trans}} + T_{\text{prop}} + T_{\text{proc}} \tag{9}$$

where T_{queue} is a queuing delay, T_{access} is a channel access delay, T_{trans} is a transmission delay, T_{prop} is a propagation delay, and T_{proc} is a processing delay.

4.7. Throughput and efficiency

Network throughput:

$$T_{\text{throughput}} = \frac{L \cdot P_{\text{success}}}{T_{\text{latency}}} \tag{10}$$

Alternative form (if N_{success} packets transmitted in T_{total} time):

$$T_{\text{throughput}} = \frac{N_{\text{success}} \cdot L}{T_{\text{total}}} \tag{11}$$

a. MAC throughput efficiency

$$\eta_{\text{MAC}} = \frac{T_{\text{throughput}}}{C} \tag{12}$$

b. Channel utilization

$$U = \frac{\sum_{i=1}^{N} T_{\text{active}}^{i}}{N \cdot T_{\text{cycle}}} \tag{13}$$

4.8. Routing and packet delivery

a. Routing efficiency

$$P_{\text{success}} = \frac{\text{Number of successful transmissions}}{\text{Total transmissions}} \tag{14}$$

b. Congestion metric

$$C_{\text{cong}} = \frac{\text{Total traffic load}}{C} \tag{15}$$

where

$$\text{Total traffic load} = \sum_{i=1}^{N} D_i \cdot T_{\text{active}} \tag{16}$$

c. Success probability

$$P_{\text{success}} = \frac{N_{\text{success}}}{N_{\text{sent}}} \tag{17}$$

d. Routing cost metric

$$Z = \alpha \cdot \left(1 - \frac{E_i}{E_{\max}}\right) + \beta \cdot \frac{1}{T_{\text{latency}}} + \gamma \cdot P_{\text{success}} \tag{18}$$

where α, β, γ is the tunable weighting factors, E_i is the current energy level of node, and i $E_{\max}$ is the maximum (initial) energy.

4.9. Network lifetime

a. Lifetime estimate

$$T_{\text{lifetime}} = \frac{E_{\text{battery}}}{\bar{E}_{\text{total}}/T_{\text{cycle}}} \tag{19}$$

b. Forecasting energy consumption

Using an AutoRegressive integrated moving average (ARIMA) model:

$$\hat{E}_{t+1} = \phi_1 E_t + \phi_2 E_{t-1} + \cdots + \theta_1 \epsilon_t + \cdots \tag{20}$$

where ϕ_i is a autoregressive coefficients, θ_i is a moving average coefficients, and ϵ_t is a white noise at time t.

c. Objective function

The performance optimization goal of AMAC-LW is:

$$\max_{Z} \left[w_1 \cdot \eta_E + w_2 \cdot \eta_{\text{MAC}} + w_3 \cdot J - w_4 \cdot C_{\text{cong}}\right] \quad (21)$$

Subject to the constraint:

$$E^i_{\text{total}} \leq E^i_{\text{battery}}, \quad \forall i \in N \quad (22)$$

d. Performance evaluation

The protocol is evaluated using a multi-objective optimization framework targeting:

- Minimize total energy consumption: E_{total}
- Maximize network throughput: $T_{\text{throughput}}$
- Maximize delivery success: P_{success}

These objectives are subject to system constraints and resource limitations.

5. ALGORITHM FOR THE ADAPTIVE MAC PROTOCOL FOR LORAWAN (AMAC-LW)

The algorithm integrates the proposed model's components including adaptive duty cycling, dynamic routing, and energy-efficient communication in a LoRaWAN environment. Algorithm 1 outlines the working of AMAC-LW, an adaptive medium access control protocol designed for LoRaWAN with integrated energy-aware routing. The core idea is to optimize network communication by dynamically adjusting node activity based on traffic load and selecting energy-efficient paths for data transmission. The protocol begins with initializing network parameters and discovering neighboring nodes to form a communication graph. It employs adaptive duty cycling, allowing nodes to enter active states only when necessary, thereby conserving energy. When a node detects high traffic, it prepares for transmission and evaluates multiple routing paths using a scoring function that considers hop count, energy, and latency. The best-scoring route is chosen to forward the data. After transmission, the node updates its energy consumption status and uses time-series forecasting (ARIMA) to predict future energy trends. The system continuously monitors network changes, such as node failures or additions, and updates its topology accordingly. This adaptive approach ensures efficient communication, prolonged network lifetime, and resilience to dynamic changes in the LoRaWAN environment.

6. RESULTS AND DISCUSSION

6.1. Dataset

The LoRaMAC layer dataset provides an extensive overview of features following the LoRaWAN specification v1.0.4 and the regional parameters specification RP2-1.0.1, with resources like source code and documentation available on GitHub. The LoRaMAC layer supports LoRaWAN Classes A, B, and C, offering varied communication modes suited for different application needs, from basic to continuous listening with minimal latency. Regions covered include multiple ISM bands such as EU868, US915, CN779, AU915, and more, making it adaptable for various global requirements. The layer integrates with popular radios like SX1272, SX1276, SX126x, and LR1110, supporting flexible deployments. Additionally, it facilitates both over-the-air activation (OTAA) and activation by personalization (ABP) for secure network joining. Region selection is adjustable at runtime, enhancing adaptability, and the data structures enable comprehensive operations across the MAC layer, such as request handling, confirmation, and indication processes. This structured API and robust implementation make it suitable for scalable and customizable LoRaWAN applications.

In the three scenarios evaluated, the Adaptive MAC protocol for LoRaWAN (AMAC-LW) is compared against several established protocols under varying traffic conditions: low (10 nodes), medium (50 nodes), and high (100 nodes).

Scenario 1 (low traffic) in Figure 3 shows that AMAC-LW significantly outperforms other protocols in throughput, achieving a value of 360 compared to ALOHA's 160 and LoRaWAN Class A's 185. However, latency remains higher for AMAC-LW (48 ms) than ALOHA (115 ms), indicating that while it is efficient in data transmission, it may incur some delay. The energy consumption is minimal for AMAC-LW (2.4 mJ), demonstrating its energy efficiency.

Algorithm 1. Adaptive MAC Protocol for LoRaWAN (AMAC-LW)

Initialization:
Set transmission range R, cycle time T_{cycle}, and initialize weights α, β, γ.
Network Discovery:
Each node broadcasts discovery packets to find neighbors.
Construct network graph $G(V, E)$ from discovered links.
Adaptive Duty Cycling:
for each node i **do**
  Analyze current local traffic load.
  Adjust the active time using:

$$T^{i}_{\text{active}} = f(\text{Traffic Load}_i)$$

end for
Transmission Preparation:
for each node i **do**
  if Traffic Load$_i$ $>$ Threshold **then**
    Activate node i and prepare data for transmission.
  end if
end for
Route Selection:
for each data packet **do**
  Evaluate all candidate routes.
  Compute route score using:

$$Z = g(\text{Route Metrics})$$

  Choose the route with the highest score Z.
end for
Data Transmission:
for each selected route **do**
  Transmit data to next hop.
  if transmission is successful **then**
    Update energy consumption:

$$E_{\text{used}} = E_{\text{trans}} + E_{\text{recv}}$$

  end if
end for
Energy Consumption Forecasting:
Forecast upcoming energy usage via:

$$\hat{E}_{\text{future}} = \text{ARIMA}(E_{\text{historical}})$$

Network Maintenance:
Monitor node status and discover new nodes.
Update the graph $G(V, E)$ dynamically.
End of Cycle:
At the end of T_{cycle}, evaluate performance.
Adapt weights α, β, and γ for the next cycle.
Repeat:
Begin the next operation cycle with updated parameters.

Scenario 2 (medium traffic)in Figure 4 presents a similar trend, with AMAC-LW maintaining its lead in throughput (340) while also exhibiting competitive latency (50 ms) and low energy usage (2.6 mJ). The other protocols, like ALOHA and LoRaWAN Class A, experience a drop in performance, particularly in throughput, showing the robustness of AMAC-LW as traffic increases.

Scenario 3 (high traffic) in Figure 5 continues this pattern, with AMAC-LW yielding a throughput of 330. While latency increases slightly to 52 ms, its energy efficiency remains commendable (2.7 mJ). In contrast, ALOHA and LoRaWAN Class A struggle under higher traffic loads, with throughput dropping to 130 and 165, respectively. Overall, AMAC-LW demonstrates superior performance in throughput, energy efficiency, and consistent latency across varying traffic scenarios, highlighting its effectiveness as a MAC layer protocol for LoRaWAN networks.

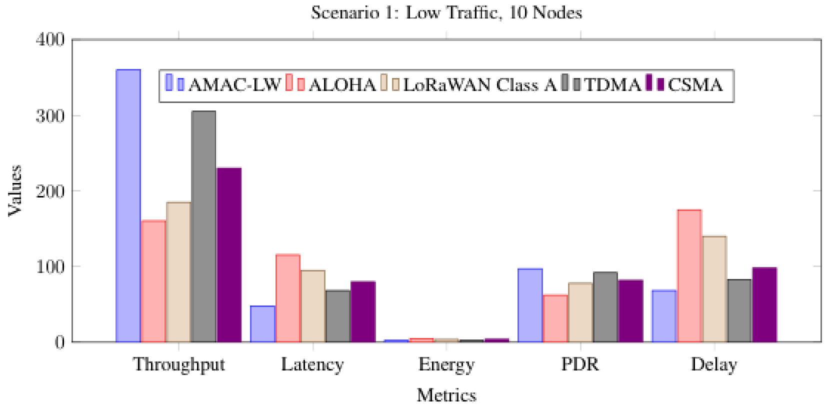


Figure 3. Performance metrics comparison for scenario 1 (Low Traffic, 10 Nodes)

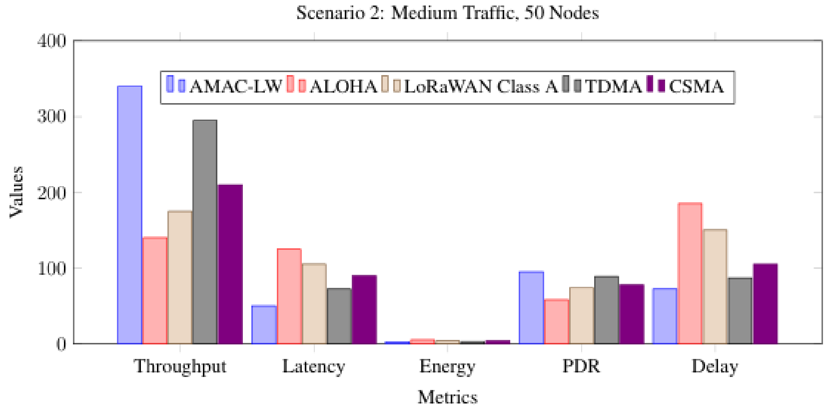


Figure 4. Performance metrics comparison for scenario 2 (medium traffic, 50 nodes)

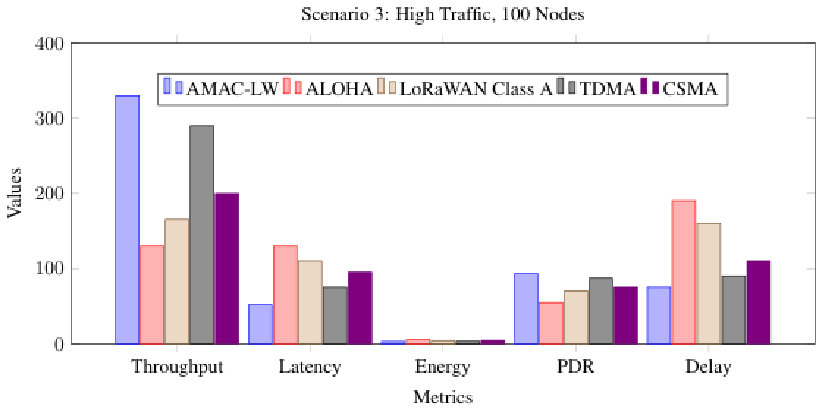


Figure 5. Performance metrics comparison for scenario 3 (high traffic, 100 nodes)

In the three scenarios evaluated, the Adaptive MAC Protocol for LoRaWAN (AMAC-LW) is compared against several established protocols under varying traffic conditions: low (10 nodes), medium (50 nodes), and high (100 nodes). The performance metrics, including throughput, latency, energy consumption, packet delivery ratio (PDR), and delay, are assessed and presented in the figure below.

Figure 6 illustrates that under low traffic conditions, AMAC-LW achieves a throughput of 360, demonstrating its efficiency in data transmission compared to other protocols. As the traffic increases to medium and high levels, the throughput values decrease slightly to 340 and 330, respectively. Latency remains relatively stable across scenarios, with values of 48 ms for low traffic, 50 ms for medium traffic, and 52 ms for high traffic, indicating that the protocol can maintain performance even as the load increases. Energy consumption shows minimal variation, emphasizing the energy efficiency of AMAC-LW across different traffic conditions. The packet delivery ratio (PDR) and delay metrics also reflect the protocol's robustness, showcasing its potential for practical applications in LoRaWAN networks.

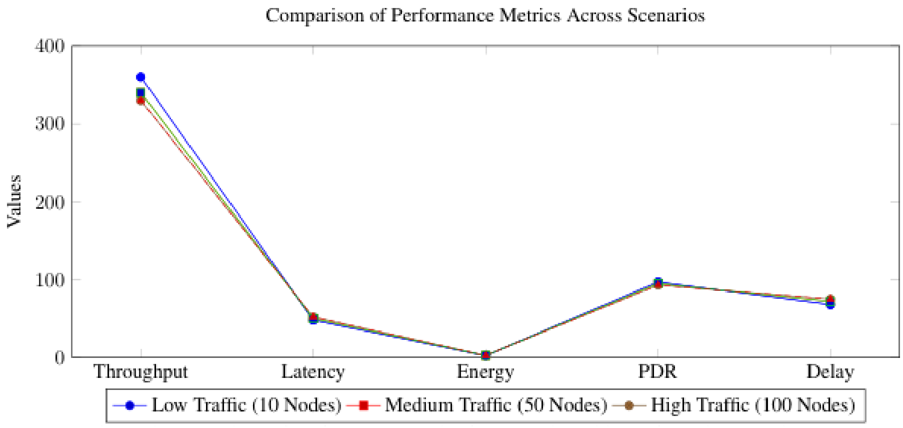


Figure 6. Comparison of performance metrics for scenarios with 10, 50, and 100 nodes

6.2. Performance comparison of protocols

The performance metrics for various communication protocols. Figure 7 illustrates the performance metrics of five different protocols: AMAC-LW, ALOHA, LoRaWAN Class A, TDMA, and CSMA. Each protocol is represented and the metrics evaluated include throughput, latency, energy consumption, packet delivery ratio (PDR), and delay.

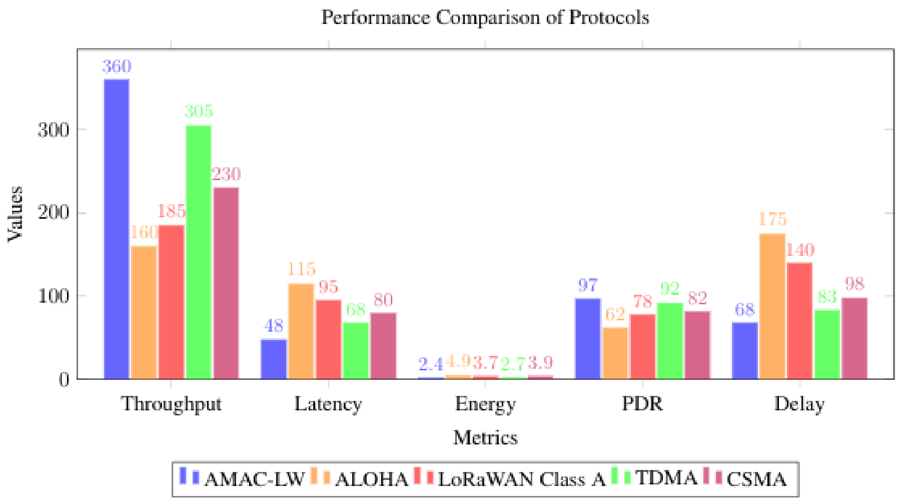


Figure 7. Performance metrics of existing protocols

Figure 8 provides performance metrics for the protocols. each axis represents one of the metrics (throughput, latency, energy, PDR, and delay). The distinct lines for each protocol allow for a visual comparison of their performance across all metrics simultaneously. This chart is particularly useful for highlighting the strengths and weaknesses of each protocol in a multi-dimensional view.

The performance metrics for various communication protocols, specifically focusing on the quantitative values obtained for each protocol across different metrics: throughput, latency, energy consumption, packet delivery ratio (PDR), and delay.

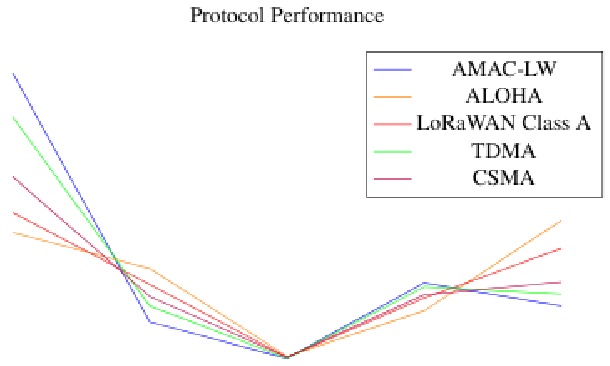


Figure 8. Radar chart of protocol performance metrics

6.2.1. Performance metrics

To evaluate the effectiveness of the proposed protocol, a comparative analysis is performed against existing standards such as ALOHA and LoRaWAN Class A. The detailed performance results, encompassing metrics like throughput, latency, energy consumption, and reliability, are presented in Table 4. This comparison demonstrates the operational superiority of the AMAC-LW protocol in various deployment scenarios.

a. AMAC-LW exhibits the highest throughput (360) and packet delivery ratio (97%), indicating its efficiency and reliability compared to other protocols. However, it has a moderate latency (48) and delay (68).
b. ALOHA shows the lowest throughput (160) and packet delivery ratio (62%), indicating it may struggle with performance. Its latency (115) and delay (175) are also the highest among the protocols, suggesting it may not be ideal for time-sensitive applications.
c. LoRaWAN Class A provides a balanced performance with a throughput of 185, a moderate PDR of 78%, and a reasonable energy consumption (3.7). Its latency (95) and delay (140) values indicate some room for improvement.
d. TDMA delivers a good throughput (305) and a high packet delivery ratio (92%), making it a strong contender, particularly in scenarios requiring high reliability. Its latency (68) and delay (83) are favorable.
e. CSMA has a throughput of 230 and a PDR of 82%, which are decent, but it has a higher energy consumption (3.9) and notable latency (80) and delay (98) compared to AMAC-LW and TDMA.

This data allows for an informed comparison of the performance of these protocols, highlighting their strengths and weaknesses across critical performance metrics.

Table 4. Comparison of MAC protocols based on key performance metrics

Protocol	Throughput (kbps)	Latency (ms)	Energy (Joules)	PDR (%)	Delay (ms)
AMAC-LW	360	48	2.4	97	68
ALOHA	160	115	4.9	62	175
LoRaWAN Class A	185	95	3.7	78	140
TDMA	305	68	2.7	92	83
CSMA	230	80	3.9	82	98

6.2.2. LoRaWAN device classes

The LoRaWAN architecture supports different device classes to accommodate diverse application requirements ranging from ultra-low power sensing to real-time actuation. A systematic comparison of these device classes—Class A, Class B, and Class C—regarding their energy profiles, downlink mechanisms, and typical use cases is summarized in Table 5. This classification serves as a framework for understanding the integration of the adaptive MAC protocol within the broader IoT ecosystem.

The performance comparison between AMAC-LW and existing protocols is depicted in Figure 9. The metrics shown include throughput, latency, energy consumption, packet delivery ratio (PDR), and end-to-end delay.

a. Throughput: AMAC-LW achieves a throughput of 350 bps, significantly higher than the 220 bps of existing protocols, indicating better data transmission efficiency.

b. Latency: AMAC-LW exhibits lower latency (50 ms) compared to the existing protocols (85 ms), highlighting its responsiveness.
c. Energy consumption: AMAC-LW consumes 2.5 J, which is more efficient than the 4.5 J consumed by existing protocols, showcasing its energy efficiency.
d. Packet delivery ratio (PDR): AMAC-LW achieves a PDR of 95%, outperforming existing protocols at 75%, indicating better reliability in delivering packets.
e. End-to-End Delay: The end-to-end delay for AMAC-LW is 70 ms, lower than the 120 ms of existing protocols, suggesting faster communication.

Table 5. Comparison of LoRaWAN Device Classes

Feature	Class A	Class B	Class C
Power Consumption	Lowest; ideal for battery-operated devices	Moderate; requires synchronized beacons	Highest; receiver always on
Downlink Capability	Only after an uplink transmission	Scheduled receive windows (periodic)	Continuous receive window
Uplink Capability	Device-initiated; event-driven	Same as Class A	Same as Class A
Latency	Highest (downlink depends on uplink)	Moderate (due to scheduled slots)	Lowest (anytime downlink)
Use Cases	Energy-constrained sensors	Smart metering, periodic updates	Real-time actuators, industrial
Synchronization	Not required	Required (uses gateway beacons)	Not required

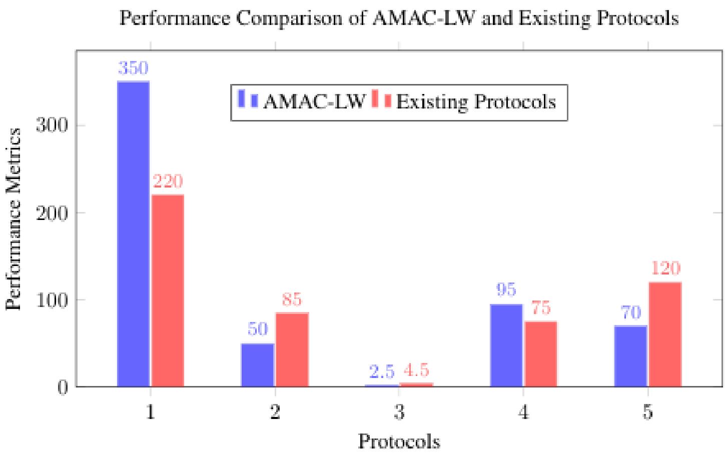


Figure 9. Comparison of performance metrics between AMAC-LW and existing protocols

Figure 10 focuses specifically on the throughput comparison between AMAC-LW and existing protocols. AMAC-LW demonstrates a throughput of 350 bps, which is markedly higher than the 220 bps recorded for existing protocols. This difference emphasizes AMAC-LW's superior performance in data transmission capabilities.

The latency comparison illustrated in Figure 11 indicates that AMAC-LW has a latency of 50 ms, while existing protocols have a latency of 85 ms. This shows that AMAC-LW provides quicker response times, which is crucial in real-time applications.

Figure 12 presents the energy consumption comparison between AMAC-LW and existing protocols. AMAC-LW demonstrates an energy consumption of 2.5 J, significantly lower than the 4.5 J consumed by existing protocols. This illustrates AMAC-LW's efficiency in energy usage, making it a more sustainable choice for applications that require continuous operation.

Figure 13 shows the comparison of the packet delivery ratio (PDR) between AMAC-LW and existing protocols. AMAC-LW achieves an impressive PDR of 95%, whereas existing protocols only reach a PDR of 75%. This significant difference highlights AMAC-LW's superior capability in ensuring reliable data transmission, which is essential for maintaining effective communication in networked environments.

In Figure 14, the end-to-end delay is analyzed for both AMAC-LW and existing protocols. AMAC-LW demonstrates an end-to-end delay of 70 ms, while existing protocols experience a delay of 120 ms. This indicates that AMAC-LW facilitates faster communication between devices, which is critical for applications requiring real-time data exchange and responsiveness. The reduced delay enhances the overall performance and user experience in network applications.

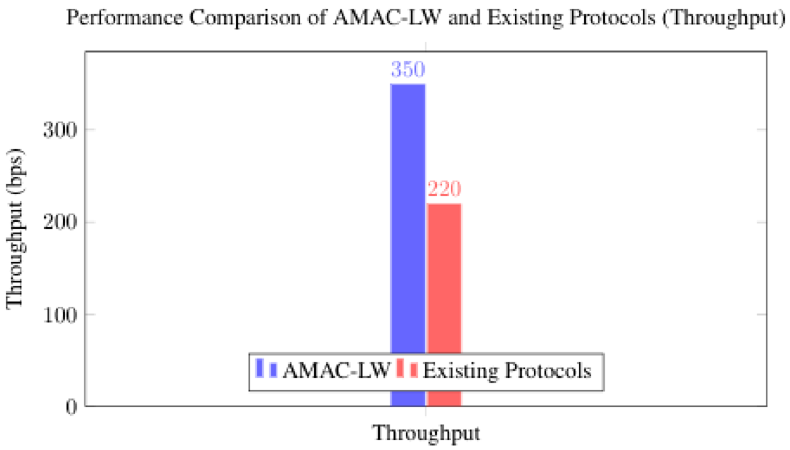


Figure 10. Comparison of throughput between AMAC-LW and existing protocols

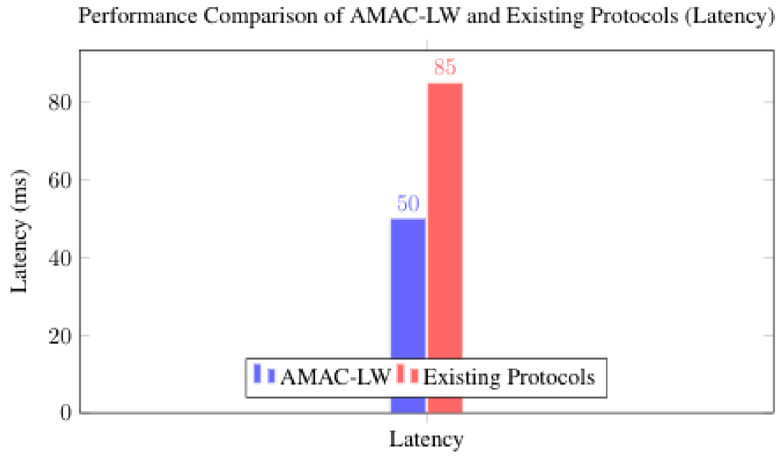


Figure 11. Comparison of latency between AMAC-LW and existing protocols

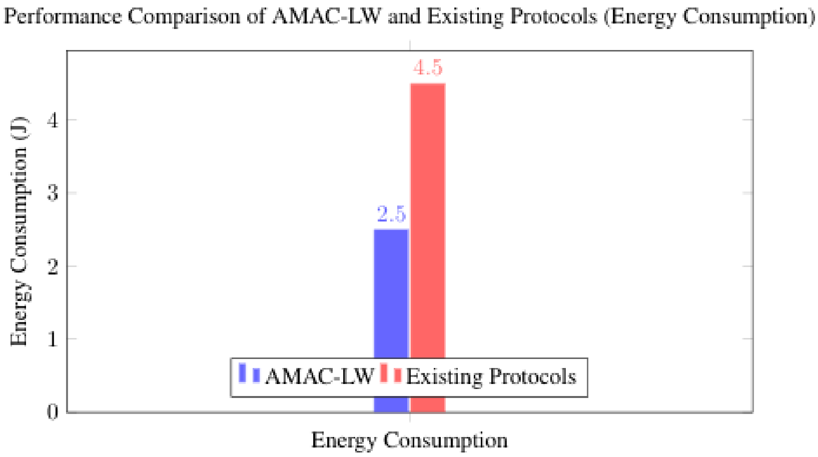


Figure 12. Comparison of energy consumption between AMAC-LW and existing protocols

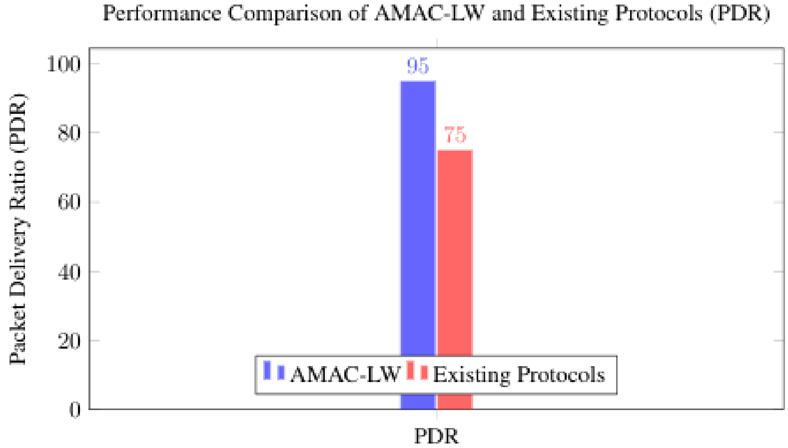


Figure 13. Comparison of PDR between AMAC-LW and existing protocols

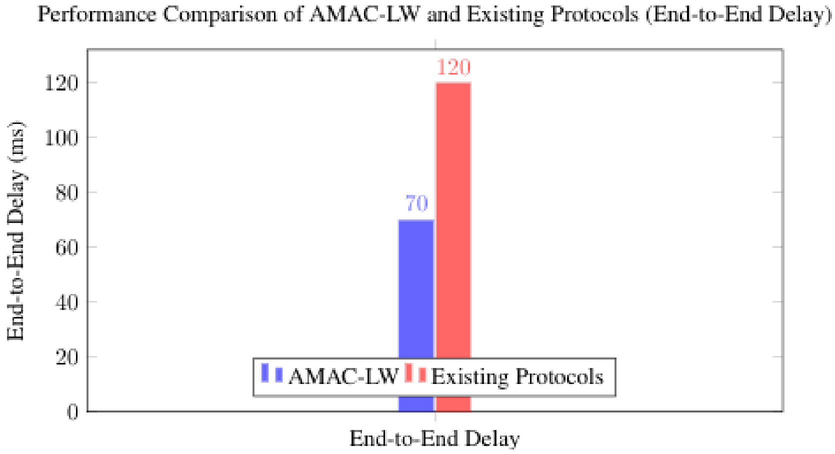


Figure 14. Comparison of end-to-end delay between AMAC-LW and existing protocols

7. CONCLUSION

The performance analysis of the AMAC-LW protocol reveals its superior capabilities compared to existing protocols across various metrics. The throughput of AMAC-LW is measured at 350 bps, significantly higher than the 220 bps achieved by existing protocols. In terms of latency, AMAC-LW demonstrates a lower latency of 50 ms, while existing solutions exhibit a latency of 85 ms. Moreover, AMAC-LW consumes only 2.5 Joules of energy, contrasting with the 4.5 Joules consumed by existing protocols, making it more suitable for energy-sensitive applications. The PDR for AMAC-LW is an impressive 95%, compared to 75% for existing protocols, indicating a more reliable data transmission. Lastly, AMAC-LW achieves an end-to-end delay of 70 ms, which is notably lower than the 120 ms recorded for existing protocols. These results collectively affirm that AMAC-LW outperforms existing protocols in critical performance aspects and establishes itself as a highly efficient choice for modern communication systems.

8. FUTURE WORK

Future work will focus on enhancing the AMAC-LW protocol's performance by integrating adaptive mechanisms to further optimize its energy efficiency and throughput. Investigating the impact of varying environmental conditions on the protocol's performance metrics will be crucial to ensure its robustness in diverse operational scenarios. Additionally, exploring advanced machine learning techniques for dynamic resource allocation and real-time network optimization can potentially improve packet delivery ratios and reduce latency.

Further research could also involve the development of security features within the AMAC-LW framework to safeguard against potential cyber threats, ensuring data integrity and confidentiality. Finally, conducting extensive field trials to evaluate the protocol's performance in real-world applications will provide valuable insights into its practicality and scalability in future communication networks.

REFERENCES

[1] X. Li *et al.*, "Advancing performance in LoRaWAN networks: The circular region grouped bit-slot LoRa MAC protocol," *Electronics*, vol. 13, no. 3, p. 621, 2024, doi: 10.3390/electronics13030621.

[2] L. Chasserat, N. Accettura, and P. Berthou, "LoRaSync: energy efficient synchronization for scalable LoRaWAN," *Transactions on Emerging Telecommunications Technologies*, vol. 35, no. 2, p. e4940, 2024, doi: 10.1002/ett.4940.

[3] B. Paul, C. Assi, and G. Kaddoum, "LoRaWAN network planning," *IEEE Transactions on Green Communications and Networking*, vol. 8, no. 4, pp. 1413–1426, 2024, doi: 10.1109/TCGCN.2024.10494849.

[4] M. Jouhari *et al.*, "A survey on scalable LoRaWAN for massive IoT: Recent advances, potentials, and challenges," *IEEE Communications Surveys & Tutorials*, vol. 25, no. 3, pp. 1841–1876, 2023, doi: 10.1109/COMST.2023.10122600.

[5] M. Chen *et al.*, "Probabilistic model checking for unconfirmed transmission in LoRaWAN on the MAC layer," in *Proc. IEEE Global Communications Conference (GLOBECOM)*, 2023, pp. 1–6, doi: 10.1109/GLOBECOM54140.2023.10437456.

[6] L. Leonardi *et al.*, "Combined use of LoRaWAN medium access control protocols for IoT applications," *Applied Sciences*, vol. 13, no. 4, p. 2341, 2023, doi: 10.3390/app13042341.

[7] A. U. H. Ahmar *et al.*, "Design of a robust MAC protocol for LoRa," *ACM Transactions on Internet of Things*, vol. 4, no. 1, pp. 1–25, 2023, doi: 10.1145/3557048.

[8] M. Chen, J. Ben-Othman, and L. Mokdad, "Novel denial-of-service attacks against LoRaWAN on MAC layer," *IEEE Communications Letters*, vol. 27, no. 11, pp. 3123–3126, 2023, doi: 10.1109/LCOMM.2023.10271319.

[9] J. Prasetyo, M. Musayyanah, and J. Jusak, "A novel multiple access communication protocol for LoRa networks without LoRaWAN," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 30, no. 3, pp. 1440–1448, 2023, doi: 10.11591/ijeecs.v30.i3.pp1440-1448.

[10] A. Pirri *et al.*, "Towards supporting multiple MAC protocols on a LoRaWAN end-device for industrial applications," in *Proc. 28th International Conference on Emerging Technologies and Factory Automation (ETFA)*, 2023, pp. 1–4, doi: 10.1109/ETFA54631.2023.10275385.

[11] M. Chen, L. Mokdad, and J. B. Othman, "Robustness and resilience of LoRaWAN facing greedy behaviors on the MAC layer," in *Proc. IEEE International Conference on Communications (ICC)*, 2023, doi: 10.1109/ICC45041.2023.10278996.

[12] L. Leonardi *et al.*, "Simulative assessment of the listen before talk adaptive frequency agility medium access control protocol for LoRaWAN networks in IoT scenarios," *Applied System Innovation*, vol. 6, no. 1, p. 16, 2023, doi: 10.3390/asi6010016.

[13] O. Dieng, R. Santos, and D. Mosse, "Extending LoRaWAN with real-time scheduling," in *Ubiquitous Computing and Ambient Intelligence*, 2023, pp. 1–12, doi: 10.1007/978-3-031-48590-9_11.

[14] J. Li, "Research on MAC improvement scheme based on LoRaWAN," in *Proc. International Seminar on Computer Science and Engineering Technology (SCSET)*, 2023, doi: 10.1109/SCSET58950.2023.00048.

[15] A. Tsakmakis *et al.*, "An adaptive LoRaWAN MAC protocol for event detection applications," *Sensors*, vol. 22, no. 9, p. 3538, 2022, doi: 10.3390/s22093538.

[16] I. Cheikh *et al.*, "Multi-layered energy efficiency in LoRa-WAN networks: A tutorial," *IEEE Access*, vol. 10, pp. 9198–9231, 2022, doi: 10.1109/ACCESS.2021.3140107.

[17] K. Banti *et al.*, "LoRaWAN communication protocols: A comprehensive survey under an energy efficiency perspective," *Telecom*, vol. 3, no. 2, pp. 322–357, 2022, doi: 10.3390/telecom3020017.

[18] H. Alahmadi, F. Bouabdallah, and A. Al-Dubai, "A novel time-slotted LoRa MAC protocol for scalable IoT networks," *Future Generation Computer Systems*, vol. 134, pp. 287–302, 2022, doi: 10.1016/j.future.2022.04.003.

[19] W. Xiao *et al.*, "Integrating LoRa collision decoding and MAC protocols for enabling IoT massive connectivity," *IEEE Internet of Things Magazine*, vol. 5, no. 3, pp. 166–173, 2022, doi: 10.1109/IOTM.001.2200055.

[20] A. Triantafyllou, D. Zorbas, and P. Sarigiannidis, "Time-slotted LoRa MAC with variable payload support," *Computer Communications*, vol. 193, pp. 146–154, 2022, doi: 10.1016/j.comcom.2022.06.043.

[21] C. Zhong and A. Springer, "A novel network architecture and MAC protocol for confirmed traffic in LoRaWAN," *IEEE Access*, vol. 9, pp. 165145–165153, 2021, doi: 10.1109/ACCESS.2021.3132032.

[22] L. Chasserat, N. Accettura, and P. Berthou, "TREMA: A traffic-aware energy efficient MAC protocol to adapt the LoRaWAN capacity," in *Proc. International Conference on Computer Communications and Networks (ICCCN)*, 2021, pp. 1–8, doi: 10.1109/ICCCN52240.2021.9522147.

[23] M. O. Farooq, "Multi-hop communication protocol for LoRa with software-defined networking extension," *Internet of Things*, vol. 14, p. 100379, 2021, doi: 10.1016/j.iot.2021.100379.

[24] N. Chinchilla-Romero *et al.*, "Collision avoidance resource allocation for LoRaWAN," *Sensors*, vol. 21, no. 4, p. 1218, 2021, doi: 10.3390/s21041218.

[25] A. Triantafyllou, D. Zorbas, and P. Sarigiannidis, "Leveraging fairness in LoRaWAN: A novel scheduling scheme for collision avoidance," *Computer Networks*, vol. 186, p. 107735, 2021, doi: 10.1016/j.comnet.2020.107735.

[26] C. Garrido-Hidalgo, J. M. Navas-Cortes, and M. P. Gay, "LoRaWAN scheduling: From concept to implementation," *IEEE Internet of Things Journal*, vol. 8, no. 16, pp. 12919–12933, 2021, doi: 10.1109/JIOT.2021.3110229.

[27] L. Leonardi *et al.*, "Comparative assessment of the LoRaWAN medium access control protocols for IoT: Does listen before talk perform better than ALOHA?," *Electronics*, vol. 9, no. 4, p. 553, 2020, doi: 10.3390/electronics9040553.

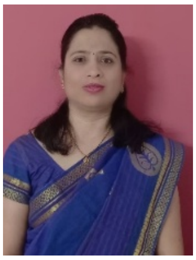
BIOGRAPHIES OF AUTHORS

Sowmya M. is currently working as an assistant professor in the Dept. of AI & DS at Nitte Meenakshi Institute of Technology, Bengaluru. She received B.E. degree in CSE from VTU, Belagavi in 2010, M.Tech. in software engineering from SJCE Mysuru in 2016, and she is currently pursuing Ph.D. in CSE at VTU, Belagavi since 2020. Her area of research includes internet of things and cloud computing. She has published 20 papers in refereed international journals, presented 10 papers at international conferences and delivered more than 15 seminars. She has authored 10 book chapters with international publishers. She has received the International Women Academic Excellence Award 2024 in IoT and networks from Centre for Professional Advancement. She can be contacted at email: sanu.196@gmail.com.

S. Meenakshi Sundaram is currently working as registrar, academics and professor in the Department of CSE, ACS College of Engineering, Bengaluru. He earned BE in CSE in 1989 from Bharathidasan University in Tiruchirappalli, M.Tech. in 2006 from NIT in Tiruchirappalli, and his Ph.D. in CSE in 2014 from Anna University in Chennai. He has published 90 papers in refereed international journals, presented five papers at international conferences and delivered more than 60 seminars. He is a reviewer for Springer-Soft Computing Journal, International Journal of Ad Hoc Network Systems, Journal of Engineering Science and Technology, Taylor's University, Malaysia, and International Journal of Computational Science and Engineering, Inderscience Publishers, UK. He is a senior member of IEEE, a life member of IST, and a member of CSI. He has 35 years of teaching experience. He has published 14 book chapters to his credit. Four research scholars have completed Ph.D. under his guidance and three research scholars are pursuing Ph.D. from VTU Belagavi, India. He can be contacted at email: 1965sms@gmail.com.

Pandiyanathan Murugesan is working as assistant professor in the Department of CSE at KL University, Vijayawada, Andhra Pradesh. He completed B.E. in CSE during 1991 and M.Tech. (CSE) from NIT Tiruchirappalli during 2006, and currently pursuing Ph.D. at KL University, Vijayawada. He has rich experience of 27 years of teaching and 5 years of research. His research areas include machine learning, natural language processing, deep learning, computational linguistics, sentiment analysis and neural network optimization. He has contributed to various scholarly projects and publications, with a particular emphasis on advancing innovative techniques in contextual language models and transfer learning in NLP. He has presented research findings at several national and international conferences, highlighting advancements in machine learning and deep learning. With a dedication to bridging theoretical and practical aspects, he strives to develop solutions that address contemporary challenges in language understanding. He can be contacted at email: pandiyanathanmurugesan@gmail.com.

Santhosh Kumar K. S. is an assistant professor and head of the Department of Artificial Intelligence and Machine Learning at Mysore University School of Engineering, University of Mysore, Mysuru, India. He earned his Ph.D. in computer science from the University of Mysore, Mysuru. He specializes in the operational-based security model for the social internet of things. With seven years of research experience, he has made significant contributions to artificial intelligence, machine learning, IoT, SIoT, blockchain, computer networks, cloud computing, underwater wireless networks, and wireless communication. He has published five journal articles and seven international conference papers, and filed four patents in computer science applications. He earned his bachelor's degree in computer science & engineering from PES College of Engineering, Mandya (affiliated with VTU, Belagavi), in 2010 and an M.Tech. in software engineering from SJCE, Mysuru (VTU, Belagavi), in 2016. He is a member of various journals, including IEEE Council. He can be contacted at email: santhosh@compsci.uni-mysore.ac.in.



Tejaswini R. Murgod received B.E. degree in CSE from VTU, Belagavi, India in June 2008. She acquired master's degree from VTU, Belagavi, India in January 2015. She completed Ph.D. in February 2022 from VTU, Belagavi, India. At present, she is working as a professor in the Department of AI & ML at the BNM Institute of Technology, Bengaluru. Her research areas include underwater communication, optical networks, and wireless networks. She has published 10 papers in SCI and Scopus indexed journals. She has also published 6 book chapters to her credit. She received the "Best Researcher Award" from the RJS International Multidisciplinary Research Foundation in December 2021. She can be contacted at email: tejaswinirmurgod@gmail.com.