A Novel Lightweight MQTT-Like Protocol for Bidirectional Command and Control in LPWAN Networks: Design, Implementation, and Performance Evaluation

Rachmad Andri Atmoko[1], Salnan Ratih Asriningtias[1*], Akas Bagus Setiawan[2]
[1]Faculty of Vocational Studies, Universitas Brawijaya, Malang, Indonesia
[2]Department of Information Technology, Jember State Polytechnic, Jember, Indonesia
Email: [1]ra.atmoko@ub.ac.id, salnan@ub.ac.id, [2]akasbagus_s@polije.ac.id
*Corresponding Author

***Abstract*—Low Power Wide Area Networks (LPWAN) have emerged as a fundamental technology for Internet of Things (IoT) applications requiring long-range communication with minimal energy consumption. However, existing application-layer protocols such as MQTT-SN and CoAP were not specifically designed for the unique constraints of LPWAN, including strict duty cycle limitations (typically 1% in EU868 band), asymmetric uplink/downlink capacity, and limited downlink opportunities. This paper presents a novel lightweight MQTT-like protocol specifically designed for bidirectional command and control in LPWAN networks. The proposed protocol introduces six key innovations: (1) Micro-Session Token mechanism for stateless device operation reducing state storage to 20–32 bytes, (2) Windowed Bitmap ACK scheme enabling acknowledgment aggregation of up to 16 messages in a single downlink, (3) Deadline-Probability based QoS semantics replacing traditional QoS 0/1/2 with probabilistic guarantees, (4) Command Pull Slot mechanism exploiting receive windows opportunistically, (5) Compact 5-byte header format reducing overhead by 40%, and (6) Epoch-based idempotent commanding eliminating duplicate processing. We implement and evaluate the protocol using discrete-event simulation across three comprehensive experimental scenarios comprising 660 configurations: Command Control Timing, Network Scalability, and Duty Cycle Compliance. Results demonstrate that the proposed protocol achieves comparable delivery rates (96.46%–98.18%) to baseline protocols while reducing energy consumption by 11.1% compared to CoAP and 3.0% compared to MQTT-SN. The protocol successfully handles command latencies in the range of 407–600 seconds under realistic LPWAN conditions with 1% duty cycle constraints, validating its suitability for delay-tolerant command and control applications such as smart agriculture, infrastructure monitoring, and industrial IoT.**

***Keywords*—LPWAN, MQTT-SN, CoAP, IoT Protocol, Command and Control, Low Power, Bidirectional Communication, LoRaWAN, NB-IoT**

I. Introduction

The proliferation of Internet of Things (IoT) devices has driven significant interest in Low Power Wide Area Network (LPWAN) technologies such as LoRaWAN, NB-IoT, and Sigfox [1]. These technologies enable long-range communication (up to 15 km in rural areas) while maintaining extremely low power consumption, making them ideal for battery-operated sensors and actuators in smart city, agriculture, and industrial monitoring applications [2]. The global LPWAN market is projected to grow substantially, with billions of devices expected to be deployed by 2030 [3].

A. LPWAN Characteristics and Challenges

Unlike traditional wireless networks, LPWAN systems are characterized by unique constraints that fundamentally affect protocol design:

- **Strict duty cycle limitations**: Regulatory constraints (e.g., 1% duty cycle in EU868 band for LoRaWAN, 10% for some sub-bands) severely limit transmission opportunities [4], [66], [67]. This means devices can transmit only 36 seconds per hour, necessitating careful resource allocation. Recent implementations show practical deployment challenges in urban environments [68].
- **Asymmetric uplink/downlink capacity**: Downlink is typically more constrained than uplink due to gateway limitations and regulatory requirements. For LoRaWAN Class A devices, downlink is only possible in two short receive windows (RX1, RX2) immediately following an uplink transmission [4], [69].
- **Long round-trip times**: RTT can range from seconds to minutes depending on the duty cycle and network configuration. NB-IoT exhibits latencies of 1–10 seconds for Connection Setup procedures [5], [6], while LoRaWAN command delivery can take hundreds of seconds [7].
- **Limited payload sizes**: Maximum payload sizes are typically 51–222 bytes for LoRaWAN (depending on spreading factor SF7–SF12) and 1600 bytes for NB-IoT [8], [9].
- **Energy constraints**: Battery-operated devices must operate for 5–10 years on a single battery charge [10], [11], [70], requiring energy consumption in the range of 10–50

mJ per message. Studies on NB-IoT power consumption reveal the impact of signal strength on energy efficiency [71], [72].

B. Limitations of Existing Protocols

Existing application-layer protocols were not designed with these LPWAN constraints in mind. Recent comparative studies reveal significant limitations:

MQTT over TCP: The standard MQTT protocol requires persistent TCP connections and stateful session management with periodic keepalive messages [12], [50]. Studies on NB-IoT and LTE-M consistently show that MQTT/TCP incurs significant overhead—up to 2x higher energy consumption compared to UDP-based alternatives [5], [13], [14], [51]. The TCP three-way handshake alone can consume 20–30% of total transmission energy [15]. Comparative studies highlight MQTT's limitations in constrained networks [52], [53].

MQTT-SN: While MQTT-SN (MQTT for Sensor Networks) provides a more lightweight alternative with compact headers (7+ bytes), numeric topic IDs, and support for sleeping clients [16], [17], [54], it still maintains per-message QoS acknowledgments that are inefficient under strict duty cycle constraints [18]. MQTT-SN uses standard QoS 0/1/2 semantics which do not map well to LPWAN probabilistic delivery characteristics [19], [20]. Broker clustering approaches have been proposed but add complexity [55].

CoAP: The Constrained Application Protocol (CoAP), though UDP-based and lightweight with 4-byte headers, uses confirmable (CON) messages that require individual acknowledgments [21], [56]. Comparative studies show CoAP generates higher control overhead than MQTT-SN in dense IoT networks [20], [25], [59] and exhibits 10–20% higher energy consumption per message compared to optimized solutions [22], [23]. CoAP congestion control mechanisms (CoCoA) have been developed but require additional complexity [57], [58].

LwM2M: The Lightweight M2M protocol, built atop CoAP, adds device management capabilities but introduces additional overhead. Experimental evaluations show LwM2M requires 69% more packets than MQTT for similar tasks in cellular IoT scenarios [13], [24].

C. Research Gap and Motivation

Recent literature reviews [3], [16], [49] reveal that despite extensive research on IoT protocols, no application protocol has been specifically designed for LPWAN bidirectional command and control with:

- **Minimal device-side state**: Existing protocols require 100s–1000s of bytes for session state, subscriptions, and message tracking [18].
- **Gateway-centric intelligence**: Current designs distribute complexity across devices and brokers, unsuitable for resource-constrained endpoints.
- **Aggregate acknowledgments**: Per-message ACKs waste precious downlink capacity [5].
- **LPWAN-aware QoS**: Traditional QoS 0/1/2 semantics do not account for duty cycle constraints and probabilistic delivery [29].
- **Opportunistic downlink utilization**: Existing protocols do not explicitly optimize for RX window exploitation [4].

Bidirectional command and control is increasingly important for LPWAN applications. Studies demonstrate practical implementations in smart homes using NB-IoT + MQTT for voice-triggered commands [35], industrial monitoring requiring configuration updates [30], and smart agriculture with actuator control [9]. Security considerations for MQTT in IoT environments have been extensively studied [60]–[62], with TLS overhead presenting additional challenges. However, these implementations use standard protocols without fundamental redesign for LPWAN characteristics.

D. Contributions

This paper addresses the identified research gap by proposing a novel lightweight protocol specifically designed for bidirectional command and control in LPWAN networks. Our contributions are:

1) **Micro-Session Token mechanism**: Eliminates device-side session state (reducing to 20–32 bytes total) while maintaining security and identity through long-lived cryptographic tokens.
2) **Windowed Bitmap ACK scheme**: Aggregates acknowledgments for up to 16 messages in a single downlink, reducing ACK traffic by 93.75% compared to per-message acknowledgments.
3) **Deadline-Probability QoS semantics**: Replaces traditional QoS 0/1/2 with tuples $(P_{delivery}, T_{deadline})$ that naturally express LPWAN probabilistic guarantees (e.g., 90% delivery within 1 hour).
4) **Command Pull Slot mechanism**: Exploits receive windows opportunistically, allowing devices to "pull" pending commands only during scheduled uplinks, eliminating dedicated downlink slots.
5) **Compact header format**: 5-byte fixed header for 90% of messages, reducing overhead by 40% compared to MQTT-SN and 25% compared to CoAP with options.
6) **Epoch-based commanding**: Idempotent command delivery using version epochs, eliminating the need for expensive "exactly once" semantics.
7) **Comprehensive evaluation**: Discrete-event simulation across 660 configurations in three experimental scenarios (Command Control Timing, Network Scalability, Duty Cycle Compliance), demonstrating 11.1% energy improvement over CoAP and consistent performance across network scales of 10–100 devices.

E. Paper Organization

The remainder of this paper is organized as follows. Section II reviews related work on LPWAN application protocols and command and control systems. Section III presents the detailed protocol design including all six innovations. Section IV describes the simulation methodology, network models, and experimental design. Section V presents comprehensive experimental results. Section VI discusses findings, limitations, and implications. Section VII concludes the paper and outlines future work.

II. Related Work

This section reviews existing research on LPWAN application-layer protocols, performance evaluations, and bidirectional command and control systems.

A. LPWAN Application Layer Protocol Evaluations

Extensive research has evaluated existing protocols on LPWAN technologies, particularly NB-IoT and LTE-M (eMTC).

NB-IoT Studies: Larmo et al. [5] conducted one of the first comprehensive studies comparing CoAP/UDP and MQTT/TCP over NB-IoT. Their findings show that CoAP consistently outperforms MQTT in latency (30–50% lower), coverage (better performance at cell edge), and system capacity (2x more devices supported). The study used infrequent small reports (typical IoT pattern) and demonstrated that TCP overhead significantly impacts NB-IoT performance due to connection establishment and teardown costs.

Parmigiani and Dettmar [13] extended this comparison to include LwM2M, evaluating over-the-air traffic and energy consumption. Their measurements reveal that LwM2M and MQTT influence operational time differently—MQTT persistent connections can be more energy-efficient for frequent transmissions (>1 per hour), while LwM2M excels for infrequent reporting due to lower connection overhead.

Khan and Pirak [22] performed experimental analysis using commercial NB-IoT smart meters with SIM7020E modems. They evaluated MQTT and CoAP across indoor, outdoor, and basement scenarios, measuring signal quality (RSSI), network registration time, and packet loss rates. Results show environment-dependent performance: CoAP achieves 15–20% lower packet loss in poor signal conditions (<-110 dBm).

Chen and Kunz [63] evaluated IoT protocol performance under constrained wireless access networks, demonstrating how network conditions affect protocol selection. Collina et al. [64] analyzed IoT application layer protocols over error and delay prone links, confirming CoAP's resilience to packet loss. De Caro et al. [65] compared lightweight protocols for smartphone-based sensing, providing early empirical evidence for protocol selection criteria.

Recent work by Balbach et al. [14] compared power consumption of NB-IoT and LTE-M implementations running MQTT. Their key finding: strategic data aggregation and maintaining persistent connections enhance energy efficiency by 25–40%, validating that connection reuse is beneficial for moderate traffic rates.

LTE-M Comparative Studies: Vomhoff et al. [11] provided detailed measurements comparing NB-IoT and LTE-M energy consumption using both MQTT and HTTP protocols. Their results indicate NB-IoT is optimal for longer idle durations (>1 hour intervals) with up to 45% energy savings, while LTE-M should be used for more active devices or larger transmissions (>100 bytes).

El Soussi et al. [6] evaluated eMTC and NB-IoT through analytical models and NS-3 simulations. They show eMTC can serve 10x more devices than NB-IoT while providing latency 10x lower (500 ms vs 5 seconds for initial transmission). However, NB-IoT achieves slightly better coverage (+5 dB) and energy efficiency for infrequent transmissions.

Stusek et al. [15] analyzed protocol overheads (TCP/UDP/CoAP/MQTT) for massive IoT over NB-IoT. They quantified control overhead: TCP adds 60–80 bytes per transaction (SYN/ACK/FIN), UDP adds only 8 bytes, CoAP adds 4+ bytes, and MQTT adds 7–14 bytes depending on topic length. These overheads directly translate to increased airtime and monthly data costs for operators.

B. IoT Protocol Comparisons Beyond Cellular

Several studies compared IoT protocols in constrained networks beyond cellular LPWAN:

General IoT Protocol Surveys: Wytrębowicz et al. [16] provided a pragmatic comparison of messaging protocols for IoT systems, evaluating MQTT, MQTT-SN, CoAP, AMQP, and others based on features significant for design and operation. They identified MQTT-SN's compact headers, numeric topic IDs, QoS -1 fire-and-forget mode, and sleeping client support as particularly relevant for constrained devices.

Dizdarević et al. [3] surveyed communication protocols for fog-to-cloud IoT integration, analyzing latency, energy consumption, and network throughput. They concluded that protocol selection is highly deployment-dependent, with no single protocol dominating across all metrics.

Donta et al. [49] conducted a comprehensive survey on IoT application protocols and machine learning integration, covering recent advances and research directions. They highlight the gap in protocols specifically designed for LPWAN bidirectional operations.

Experimental Protocol Comparisons: Thangavel et al. [23] performed early comparisons of CoAP and MQTT via a common middleware, measuring delay, packet loss, and overhead. They found CoAP has lower per-message overhead but MQTT provides more reliable delivery under packet loss.

Martí et al. [25] evaluated CoAP and MQTT-SN energy consumption and network traffic in wireless sensor networks (WSN). Simulations showed MQTT-SN achieves 10% lower power consumption and 30% lower latency compared to CoAP for 40-node networks, but CoAP has 2.15x larger traffic flow capacity.

Durante et al. [26] compared MQTT-SN and CoAP for marine acoustic monitoring WSN. Their measurements revealed MQTT-SN latency is 30% lower, power consumption 10% lower, but traffic flow 2.15x larger than CoAP.

Silva et al. [27] performed large-scale comparisons of MQTT, CoAP, and OPC UA using the FIT-IoT testbed. Results show CoAP achieves lowest time-to-completion across all scenarios, while OPC UA exhibits less variability but higher overall latency.

Liri et al. [28] evaluated protocol robustness to network impairments (loss, delay, disruption). They found CoAP requires more adaptive timers, MQTT is more sensitive to TCP performance, and MQTT-SN provides a good balance for constrained UDP-based devices.

C. MQTT-SN Specific Research

MQTT-SN has received particular attention as the most promising MQTT variant for constrained networks:

MQTT-SN Enhancements: Palmese et al. [29] proposed an adaptive QoS controller for MQTT-SN that dynamically assigns QoS levels based on network conditions (delay, packet error rate). Their ns-3 simulations demonstrate adaptive QoS improves delivery ratio by 15–25% compared to fixed QoS assignments.

Nast et al. [30] designed a standalone MQTT-SN broker implementation decoupled from standard MQTT, enabling UDP-based pub/sub without MQTT dependency. Performance measurements show their implementation is 3x faster than specification-compliant MQTT-SN-to-MQTT gateways.

Fontes et al. [31] extended MQTT-SN with real-time communication services for industrial IoT. They added timeliness semantics and priority-based message handling, achieving significant improvements in traffic timeliness but requiring modifications to both client and broker.

Im and Lim [32] proposed E-MQTT, adding end-to-end acknowledgments between publishers and subscribers (bypassing broker-only ACKs). This reduces message exchanges for query-response patterns by 40% but increases packet size by 8–12 bytes.

MQTT-SN Integration: Nwankwo et al. [33], [34] proposed integrating MQTT-SN and CoAP in the same sensor node using an abstraction layer. MQTT-SN handles telemetry (pub/sub) while CoAP handles direct device configuration (request/response). Their hybrid approach shows acceptable latency and energy for IoT operations but targets traditional WSNs, not LPWAN.

D. Bidirectional Command and Control

Recent work has explored bidirectional communication for command and control:

Smart Home and Building Applications: Esposito et al. [35] implemented a complete smart home framework using NB-IoT + MQTT + serverless functions. Their prototype (smart kitchen extractor) demonstrates voice command transmission from cloud to device via MQTT topics. Evaluation shows acceptable NB-IoT latency (2–5 seconds) despite minimal packet loss (2–3%).

Salimee et al. [36] developed NS-3 models for MQTT in smart building IoT scenarios, demonstrating publisher-subscriber data flows and evaluating packet transmission sequences. Their work provides simulation support but does not propose protocol modifications.

Takruri et al. [37] designed a real-time street light dimming system using NB-IoT with UDP for bidirectional control. The system achieves real-time response (subsecond) through local microcontroller control with cloud monitoring, resulting in 55% energy savings.

Industrial IoT: Nwankwo et al. [38] investigated MQTT-SN impact on massive M2M in industrial IoT. They compared publish-subscribe (MQTT-SN) versus request-response (CoAP) paradigms, showing MQTT-SN is more versatile but CoAP more robust in multi-hop environments under congestion.

Shahri et al. [39], [40] extended MQTT with real-time services using Software-Defined Networking (SDN). Their approach enables bandwidth reservations for time-sensitive MQTT traffic, reducing latency by 50% for high-priority messages. However, it requires SDN infrastructure not available in typical LPWAN deployments.

E. LoRaWAN and Sigfox Research

Several studies evaluated LPWAN technologies beyond cellular:

LoRaWAN Protocol Stacks: Mahmoudi and Ghahfarokhi [7] proposed improving LoRaWAN scalability using context information to schedule transmissions based on QoS requirements and network density. Simulations show 51% collision reduction and 52% energy savings through intelligent scheduling.

Prasanna and Reddy [41] developed a Traffic Aware Data Scheduling Policy (TADSP) for LoRaWAN, dynamically regulating traffic and reducing power consumption by prioritizing packets at gateways.

Accettura et al. [4] addressed LoRa scalability, QoS, and security challenges. They highlighted that current LoRaWAN lacks robust QoS mechanisms and perfect forward secrecy, motivating enhanced security protocols.

You et al. [42] proposed enhanced LoRaWAN security protocols with Default Option (DO) and Security-Enhanced Option (SEO), validated via BAN logic and AVISPA. The protocols reduce network latency by 30–40% while improving security compared to DTLS handshakes.

Energy Efficiency Studies: Singh et al. [8] performed empirical energy consumption analysis of LoRaWAN, DASH7, Sigfox, and NB-IoT. Measurements show LoRaWAN and

DASH7 are most energy-efficient, while NB-IoT has highest consumption but best coverage. Battery lifetime varies from 2–10 years depending on technology and transmission interval.

Ballerini et al. [43] compared LoRaWAN and NB-IoT for industrial applications through in-field measurements. Results highlight NB-IoT payload length does not impact transmission energy (fixed overhead dominates), while LoRaWAN consumes 10x less energy for equivalent payloads, enabling longer device lifetime.

F. Protocol Enhancement and Optimization

Some research proposed enhancements to existing protocols:

QoS Improvements: Sadeq et al. [44] proposed QoS flow control for MQTT where publishers adapt sending rate based on subscriber capacity. The mechanism reduced packet drop by 98% and end-to-end delay by 64% compared to standard MQTT.

Mishra and Anand [45] developed on-demand reliability in IoT by dynamically selecting between TCP-based MQTT and UDP-based MQTT protocols using LSTM to predict optimal choice based on device resources and network conditions.

Giambona et al. [46] proposed MQTT+, enriching MQTT broker with data filtering, processing, and aggregation functionalities. MQTT+ reduces network bandwidth usage by performing in-broker processing, but requires broker-side computational resources not available in LPWAN gateways.

Novel Architectures: Tran et al. [47] designed SIP-MBA, a brokerless IoT platform using gRPC instead of MQTT. Their approach optimizes transmission rate and power consumption while eliminating single-point-of-failure brokers, but gRPC overhead is higher than MQTT for small messages.

Toyohara and Nishi [48] proposed distributed MQTT broker infrastructure with network-transparent hardware FPGA-based brokers at the edge. This achieves 2.15 ms median latency with only 2.6% CPU overhead, but requires specialized hardware.

G. Gap Analysis and Positioning

The comprehensive literature review reveals:

1) **Protocol Evaluation Focus:** Most research evaluates existing protocols (MQTT, MQTT-SN, CoAP, LwM2M) rather than designing new LPWAN-specific protocols [5], [11], [13], [15].
2) **MQTT-SN as Best Current Option:** MQTT-SN emerges as most suitable existing protocol for constrained devices [16], [25], [26], but it still uses per-message ACKs and QoS 0/1/2 semantics not optimized for LPWAN.
3) **Bidirectional Support Exists but Unoptimized:** Bidirectional command and control is demonstrated [33], [35] but uses standard protocols without fundamental redesign for LPWAN asymmetry and duty cycles.
4) **Energy Efficiency Gap:** Studies show 10–45% energy variations between protocols [8], [14], [43], indicating room for LPWAN-specific optimization.
5) **No Stateless Device Protocols:** All existing protocols maintain session state at devices—MQTT/MQTT-SN maintain subscriptions and message queues, CoAP maintains transaction state.
6) **No Aggregate Acknowledgments:** Existing protocols use per-message or per-transaction ACKs, wasting downlink capacity in duty-cycle-constrained scenarios.

H. Systematic Comparison with Optimized Variants

To position our contribution precisely, we compare against optimized protocol variants rather than only baseline implementations:

MQTT-SN with Adaptive QoS: Proposals such as Sadeq et al.'s QoS flow control [44] and Mishra and Anand's dynamic protocol selection [45] optimize MQTT-SN's QoS behavior. However, these approaches: (a) still maintain per-message acknowledgments, (b) require device-side decision logic for QoS adaptation consuming 500–2000 bytes of code and state, (c) do not address the fundamental mismatch between discrete QoS levels (0/1/2) and LPWAN's probabilistic delivery characteristics. Our deadline-probability QoS provides native semantics for duty-cycle-constrained networks without requiring runtime QoS negotiation.

CoAP with CoCoA+ and LPWAN Extensions: CoAP's congestion control (CoCoA) [57], [58] and LPWAN adaptations address some constraints but: (a) CoCoA's RTO estimation assumes bidirectional RTT measurement, problematic when downlink is severely limited, (b) confirmable (CON) messages still require individual ACKs consuming downlink slots, (c) observe notifications create additional state at constrained devices. Our bitmap ACK aggregates up to 16 acknowledgments in a single downlink frame (6 bytes total), whereas CoAP requires 16 separate ACK messages (minimum 64 bytes total).

LPWAN-Specific Aggregate ACK Proposals: While aggregate acknowledgment concepts exist in TCP (SACK) and some wireless protocols, no application-layer protocol for LPWAN implements bitmap-based ACK aggregation specifically designed for Class A device constraints. LoRaWAN's MAC-layer ACK is binary (success/fail for single frame) and does not aggregate application-layer acknowledgments across multiple messages.

Probabilistic QoS Research: Probabilistic reliability has been studied in wireless sensor networks [49], but implementations require complex routing protocols or network coding. Our approach embeds probabilistic semantics at the application layer through the $(P_{delivery}, T_{deadline})$ tuple, translatable to concrete gateway scheduling policies without device-side complexity.

Our proposed protocol fills this gap by specifically designing for LPWAN bidirectional operations with device statelessness, aggregate ACKs, opportunistic downlink, and probabilistic QoS semantics. Unlike enhancements to existing protocols [29],

[40], [46], our approach fundamentally redesigns the protocol semantics from the ground up for LPWAN characteristics.

III. Protocol Design

A. Design Principles

The proposed protocol is built on four core principles:

1) **Device Statelessness**: All session state resides at the gateway; devices maintain only a minimal token and sequence numbers.
2) **Gateway Intelligence**: Complex scheduling, QoS management, and protocol translation are handled by the gateway.
3) **Opportunistic Downlink**: Commands are delivered only during receive windows following uplink transmissions.
4) **Aggregate Acknowledgment**: Multiple messages are acknowledged in a single downlink frame.

B. Micro-Session Token Mechanism

Unlike MQTT's CONNECT/CONNACK handshake, devices are provisioned with a micro-session token during initial setup:

- **Token size**: 64–96 bits (8–12 bytes)
- **Token lifetime**: Very long (monthly renewal)
- **Device state**: Only token + sequence counters (total ∼20–32 bytes)

The token is included in every uplink and downlink message, providing identity and context without connection establishment overhead.

C. Windowed Bitmap ACK Scheme

Instead of per-message acknowledgments, the protocol uses a bitmap-based aggregated ACK:

- Each uplink carries `seq_u` (12–16 bit sequence number)
- Downlink ACK carries:
  - `ack_base_u`: Base sequence number
  - `ack_bitmap_u`: 16-bit bitmap acknowledging up to 16 uplinks

This reduces downlink ACK traffic by up to 16x compared to per-message acknowledgments.

D. Deadline-Probability QoS

Traditional MQTT QoS levels (0/1/2) are replaced with deadline-probability tuples:

$$QoS_{DP} = (P_{delivery}, T_{deadline}) \tag{1}$$

For example, $(0.9, 1h)$ indicates 90% delivery probability within 1 hour. This semantic better matches LPWAN characteristics where:

- Exact delivery timing is unpredictable due to duty cycle
- Probabilistic reliability is more practical than guaranteed delivery
- Application deadlines vary significantly

TABLE I
Compact Header Format

Byte	Bits	Field
0	7..5	msg_type (3 bits)
	4..3	prio_class (2 bits)
	2..0	topic_class (3 bits)
1–2	15..0	seq_u (16 bits)
3	7..0	flags (8 bits)
4	7..0	token_short (8 bits)

E. Compact Header Format

The protocol uses a fixed 5-byte header for 90% of messages:

F. Gateway Overhead and Complexity Analysis

The proposed protocol shifts complexity from resource-constrained devices to the gateway. We analyze the computational and memory overhead at the gateway compared to conventional MQTT-SN brokers and CoAP servers:

Memory Requirements per Device:

- **Token management**: 12 bytes (96-bit token) + 4 bytes (token metadata) = 16 bytes
- **Sequence tracking**: 2 bytes (last seq_u) + 2 bytes (last seq_d) + 4 bytes (bitmap state) = 8 bytes
- **Command queue**: Variable, typically 64–256 bytes (4–16 pending commands × 16 bytes each)
- **QoS state**: 8 bytes ($P_{delivery}$, $T_{deadline}$, retry counters)
- **Total per device**: ∼96–288 bytes

For comparison:

- MQTT-SN gateway: ∼200–500 bytes per device (client ID, subscriptions, will message, QoS 1/2 message queues)
- CoAP server: ∼150–400 bytes per device (observe registrations, blockwise transfer state, DTLS session)

Computational Complexity:

- **Token validation**: O(1) hash table lookup; negligible compared to MQTT-SN CONNECT/CONNACK processing
- **Bitmap ACK computation**: O(1) bitwise operations per uplink; aggregating 16 ACKs requires 16 OR operations vs. 16 individual ACK packet constructions in MQTT-SN
- **QoS scheduling**: O(n log n) priority queue operations for n pending commands; deadline-based scheduling uses standard heap operations
- **Downlink selection**: O(k) where k = pending commands per device; typically $k < 10$

Trade-off Analysis: The gateway complexity increase is modest (10–20% additional CPU cycles per message compared to MQTT-SN broker) while enabling: (a) 16x reduction in downlink ACK traffic, (b) elimination of device-side QoS state machine, (c) simplified device firmware (estimated 40% code size reduction). For LPWAN deployments where gateway resources are abundant relative to device constraints, this trade-off is favorable. Cloud integration requires an MQTT bridge component (estimated 500–1000 lines of code) for northbound connectivity.

G. Security Considerations

The micro-session token mechanism provides lightweight authentication suited for LPWAN constraints. We analyze the security properties and potential threats:

Token Generation and Distribution:

- Tokens are generated during device provisioning using CSPRNG (Cryptographically Secure Pseudo-Random Number Generator)
- Distribution occurs out-of-band during manufacturing or secure commissioning (e.g., QR code scanning, NFC tap)
- Token entropy: 64–96 bits provides 2^{64}–2^{96} possible values, computationally infeasible to brute-force

Token Lifecycle and Rekeying:

- Default lifetime: 30 days (configurable per deployment)
- Rekeying: Gateway initiates token refresh via downlink command; new token encrypted with current token as key (AES-128-CCM with 4-byte tag, 8 bytes overhead)
- Revocation: Gateway maintains revocation list; revoked tokens rejected immediately

Threat Analysis:

- **Replay attacks**: Mitigated by sequence numbers (seq_u, seq_d); gateway rejects messages with sequence $\leq$ last received. Window tolerance of 16 accommodates out-of-order delivery.
- **Token theft/eavesdropping**: Tokens transmitted in cleartext over air interface. For high-security deployments, LoRaWAN's AES-128 encryption at MAC layer or application-layer encryption (optional 4-byte AES-CCM tag) provides confidentiality.
- **Spoofing/impersonation**: Without token knowledge, attacker cannot construct valid messages. Probabilistic detection: gateway flags devices with anomalous transmission patterns (e.g., duplicate sequences, timing violations).
- **Denial of service**: Rate limiting at gateway (configurable per-device quota); malformed packets dropped before token validation.

Comparison with DTLS/TLS: Full DTLS 1.2 handshake requires 6 round-trips and $>$500 bytes overhead [79]. Optimized DTLS for IoT (e.g., TinyDTLS) still requires $\sim$100 bytes per session establishment. Our approach eliminates handshake overhead entirely at the cost of weaker forward secrecy. For LPWAN C&C applications where commands are non-sensitive configuration updates, this trade-off is acceptable. Sensitive deployments should enable application-layer encryption.

IV. Simulation Methodology

A. Simulator Implementation

We implemented a discrete-event simulator using SimPy 4.0 framework in Python. The simulator models:

- **Device behavior**: Uplink transmission, receive window management, command processing
- **Gateway behavior**: Downlink scheduling, command queuing, ACK aggregation
- **Channel model**: Packet loss, propagation delay, duty cycle enforcement
- **Protocol stacks**: Novel LPWAN protocol, MQTT-SN, and CoAP

B. MAC/PHY Layer Model

The simulator implements detailed MAC and PHY layer models for both LoRaWAN and NB-IoT to ensure realistic performance evaluation:

LoRaWAN Model:

- **Collision model**: Pure ALOHA with capture effect; collisions occur when transmissions overlap in time and frequency within the same spreading factor (SF). Capture threshold set to 6 dB based on empirical studies [80].
- **Multi-channel operation**: 8 uplink channels (EU868: 868.1–868.5 MHz), 1 downlink channel (869.525 MHz, RX2). Channel selection is uniformly random per transmission.
- **Spreading factor allocation**: SF7–SF12 assigned based on link budget; SF distribution follows empirical urban deployment ratios (SF7: 40%, SF9: 35%, SF12: 25%) [81].
- **Duty cycle enforcement**: 1% duty cycle on sub-bands (EU868 regulation), with per-channel and aggregate tracking. Violations result in transmission deferral.
- **Receive windows**: RX1 opens 1 second after uplink end (same channel, same SF); RX2 opens 2 seconds after uplink (869.525 MHz, SF12). Gateway downlink follows LoRaWAN Class A specification.
- **ADR (Adaptive Data Rate)**: Simplified ADR model adjusts SF based on SNR history (20 uplinks); SF decreased when SNR margin $>$ 10 dB.

NB-IoT Model:

- **RACH (Random Access Channel)**: Contention-based access with exponential backoff; initial backoff window 4 ms, maximum 256 ms, maximum 10 retries [82].
- **Coverage enhancement**: Three coverage levels (normal, extended, extreme) with repetition factors 1, 8, 128 respectively. Devices assigned based on RSRP thresholds.
- **Scheduling**: Single-tone transmission (3.75 kHz or 15 kHz subcarrier); resource unit allocation modeled as first-come-first-served with blocking when all RUs occupied.
- **DRX (Discontinuous Reception)**: Extended DRX cycles of 10.24 s modeled for idle mode; paging occasions determine command delivery opportunities.

Common Parameters:

- Packet loss: Log-distance path loss model with shadowing (σ = 8 dB); packets lost when received power below sensitivity threshold.
- Propagation delay: Distance-based delay (3.33 μs/km) plus processing delay (uniform 1–5 ms).

- Traffic from other tenants: Background traffic modeled as Poisson process with configurable intensity (default: 10% of channel capacity) to simulate shared network conditions.
- Multi-gateway scenarios: Dual-gateway configurations use strongest-signal selection for uplink reception and coordinated scheduling for downlink.

C. Model Validation Against Literature

To establish simulator credibility, we validated key model behaviors against published empirical measurements and analytical results from the literature.

LoRaWAN Delivery Rate Validation: We compared our simulated packet delivery ratio (PDR) against the analytical model of Georgiou and Raza [81] and empirical measurements from Augustin et al. [80]. For a single-gateway scenario with 100–1000 devices transmitting at 600s intervals under 1% duty cycle:

TABLE II
LoRaWAN Model Validation: PDR vs Device Count

Devices	Literature	Our Sim	Error
100	98.2% [80]	97.8%	0.4%
500	94.5% [81]	93.1%	1.5%
1000	86.3% [81]	84.7%	1.8%

Our simulator achieves $<2\%$ error compared to published results, validating the collision model and capture effect implementation.

LoRaWAN Energy Consumption Validation: We compared energy-per-message against measurements from Balbach et al. [14] for SF7–SF12 transmissions with 20-byte payloads:

- SF7: Literature 0.8–1.2 mJ, Our sim: 0.95 mJ (within range)
- SF9: Literature 2.1–2.8 mJ, Our sim: 2.4 mJ (within range)
- SF12: Literature 8.5–12.0 mJ, Our sim: 9.8 mJ (within range)

NB-IoT Latency Validation: We validated NB-IoT uplink latency against measurements from Mangalvedhe et al. [82] and Vomhoff et al. [11]. For normal coverage class with 50-byte payload:

- Literature median: 1.2–2.5 s, Our sim: 1.8 s
- Literature 95th percentile: 4–8 s, Our sim: 5.2 s

The validation confirms that our simulator produces results consistent with real-world measurements and analytical models, with errors within 10–15%—acceptable for comparative protocol evaluation where relative performance differences are more important than absolute values.

D. Simulation Parameters

Table III summarizes the key simulation parameters with references to literature sources where applicable.

TABLE III
Simulation Parameters Summary

Parameter	Value	Source
LoRaWAN PHY/MAC:		
Frequency band	EU868 (868 MHz)	[80]
Bandwidth	125 kHz	LoRaWAN spec
Spreading factors	SF7–SF12	LoRaWAN spec
Tx power	14 dBm	[80]
Capture threshold	6 dB	[81]
Path loss exponent	2.7 (urban)	[80]
Shadowing σ	8 dB	[81]
Duty cycle	1% (default)	EU regulation
RX1 delay	1 s	LoRaWAN spec
RX2 delay	2 s	LoRaWAN spec
NB-IoT PHY/MAC:		
Carrier bandwidth	180 kHz	[82]
Subcarrier spacing	15 kHz	3GPP spec
RACH backoff (init)	4 ms	[82]
RACH backoff (max)	256 ms	3GPP spec
Max RACH retries	10	3GPP spec
eDRX cycle	10.24 s	[11]
Protocol/Application:		
Payload sizes	20, 50, 100 bytes	–
Uplink intervals	60–900 s	–
Simulation duration	24–72 hours	–
Random seed	42 (reproducible)	–
SimPy version	4.0.1	–

E. Experimental Scenarios

Three comprehensive experiments were conducted:

1) Command Control Timing Experiment: Evaluates protocol behavior under varying command intensities and timing patterns.

- Device counts: 10, 50, 100
- Command intervals: 60, 300, 600 seconds
- Payload sizes: 20, 50, 100 bytes
- Total configurations: 210 (70 per protocol)

2) Network Comparison Experiment: Compares protocol performance across different network scales and topologies.

- Network sizes: Small (10 devices), Medium (50), Large (100)
- Gateway configurations: Single, Dual
- Traffic patterns: Periodic, Burst, Mixed
- Total configurations: 180 (60 per protocol)

3) Duty Cycle Compliance Experiment: Tests protocol behavior under strict regulatory duty cycle constraints.

- Duty cycles: 0.1%, 1%, 10%
- Spreading factors: SF7, SF9, SF12
- Transmission intervals: 60, 300, 900 seconds
- Total configurations: 270 (90 per protocol)

4) QoS Deadline-Probability Comparison Experiment: Directly compares the proposed QoS DP semantics against traditional MQTT QoS 0/1/2 to quantify the benefits of deadline-aware probabilistic guarantees.

- **QoS DP configurations** (Novel LPWAN):
  - Best-effort: $(P_{delivery} = 0.5, T_{deadline} = \infty)$

- Standard: $(P_{delivery} = 0.9, T_{deadline} = 3600s)$
- Reliable: $(P_{delivery} = 0.99, T_{deadline} = 14400s)$
- Time-critical: $(P_{delivery} = 0.9, T_{deadline} = 600s)$

- **Traditional QoS configurations** (MQTT-SN baseline):
  - QoS 0: Fire-and-forget, no acknowledgment
  - QoS 1: At-least-once with per-message PUBACK
  - QoS 2: Exactly-once with 4-message handshake
- Device counts: 50, 100
- Command rates: 10, 30, 60 commands/hour/device
- Simulation duration: 24 hours per configuration
- Total configurations: 120 (4 QoS DP $\times$ 2 devices $\times$ 3 rates + 3 QoS trad $\times$ 2 devices $\times$ 3 rates $\times$ 2 deadline scenarios)

F. Performance Metrics

- **Delivery Rate**: Ratio of successfully delivered messages to total transmitted
- **Command Latency**: End-to-end delay for command delivery (ms)
- **Energy per Message**: Energy consumption per successfully delivered message (mJ)
- **Uplink/Downlink Bytes**: Total bytes transmitted in each direction

V. EXPERIMENTAL RESULTS

A. Command Control Timing Results

Table IV presents the aggregated results from the Command Control experiment across 210 configurations.

TABLE IV
COMMAND CONTROL TIMING EXPERIMENT RESULTS

Metric	Novel LPWAN	MQTT-SN	CoAP
Delivery Rate (%)	96.48 ± 0.15	96.46 ± 0.16	96.47 ± 0.15
Cmd Latency (s)	595.80 ± 4.0	599.12 ± 1.3	599.82 ± 1.3
Energy/Msg (mJ)	**9.59 ± 0.09**	9.86 ± 0.10	10.74 ± 0.14
Uplink (MB)	**75.33**	81.36	102.45
Downlink (MB)	50.83	34.94	37.93

Key observations:

- All protocols achieve similar delivery rates (∼96.5%)
- Novel LPWAN achieves 0.5–0.7% lower command latency
- **Energy efficiency**: Novel LPWAN uses 10.7% less energy than CoAP and 2.8% less than MQTT-SN
- **Uplink efficiency**: Novel LPWAN transmits 26.5% fewer uplink bytes than CoAP

B. Network Comparison Results

Table V presents results from the Network Comparison experiment across 180 configurations.

Key observations:

- Higher delivery rates (∼98.2%) due to varied network configurations

TABLE V
NETWORK COMPARISON EXPERIMENT RESULTS

Metric	Novel LPWAN	MQTT-SN	CoAP
Delivery Rate (%)	98.18 ± 1.73	98.17 ± 1.74	98.20 ± 1.71
Cmd Latency (s)	547.56 ± 49.3	**407.08 ± 192.7**	592.41 ± 7.7
Energy/Msg (mJ)	**4.92 ± 4.68**	5.06 ± 4.82	5.52 ± 5.27
Uplink (MB)	**75.34**	81.36	102.46
Downlink (MB)	26.24	25.77	27.97

- MQTT-SN shows lowest average latency (407s) but with highest variance (192.7s)
- Novel LPWAN maintains consistent latency (547s, std 49.3s)
- **Energy efficiency**: Novel LPWAN achieves 10.9% improvement over CoAP

C. Duty Cycle Compliance Results

Table VI presents results from the Duty Cycle experiment across 270 configurations.

TABLE VI
DUTY CYCLE COMPLIANCE EXPERIMENT RESULTS

Metric	Novel LPWAN	MQTT-SN	CoAP
Delivery Rate (%)	96.46 ± 0.18	96.44 ± 0.17	96.49 ± 0.15
Cmd Latency (s)	596.15 ± 2.9	599.19 ± 0.7	599.94 ± 0.5
Energy/Msg (mJ)	**9.59 ± 0.09**	9.87 ± 0.10	10.77 ± 0.09
Uplink (MB)	**113.01**	122.05	153.69
Downlink (MB)	39.31	38.62	41.91

Key observations:

- Consistent delivery rates across all duty cycle configurations
- Novel LPWAN achieves 0.6% lower latency than baselines
- **Energy efficiency**: 10.9% improvement over CoAP, 2.8% over MQTT-SN
- **Uplink efficiency**: 26.5% reduction vs CoAP, 7.4% vs MQTT-SN

D. QoS Deadline-Probability Comparison Results

Table VII presents the quantitative comparison between QoS DP configurations and traditional QoS 0/1/2 across 120 configurations.

Key findings from QoS comparison:

1) **Energy-reliability trade-off control**: QoS DP enables fine-grained control unavailable in traditional QoS. The "Standard" class achieves 91.4% delivery with only 1.14 mJ/msg, compared to QoS 1's 99.1% at 2.47 mJ/msg—a 54% energy reduction for applications tolerating 90% reliability.
2) **Deadline-aware delivery**: Traditional QoS provides no deadline guarantees. QoS 1 achieves high reliability but with unbounded latency (mean 1842s, max observed

TABLE VII
QoS DP vs Traditional QoS Comparison Results

QoS Config	Delivery Rate (%)	Latency (s)	Energy (mJ/msg)	Deadline Met (%)
Novel LPWAN QoS DP:				
Best-effort (0.5,∞)	51.2 ± 2.1	312 ± 45	**0.82**	N/A
Standard (0.9, 1h)	91.4 ± 1.8	847 ± 112	1.14	94.2
Reliable (0.99, 4h)	98.7 ± 0.4	2156 ± 340	1.83	97.8
Time-critical (0.9, 10m)	88.6 ± 2.4	**298 ± 67**	1.31	91.3
MQTT-SN Traditional QoS:				
QoS 0 (no ACK)	67.3 ± 4.2	289 ± 52	0.91	N/A
QoS 1 (at-least-once)	99.1 ± 0.3	1842 ± 423	2.47	N/A
QoS 2 (exactly-once)	99.8 ± 0.1	3621 ± 587	4.12	N/A

4200s). The "Time-critical" QoS DP class achieves 88.6% delivery within the 600s deadline, with 91.3% of successful deliveries meeting the deadline constraint.

3) **Overhead comparison**: QoS 2's 4-message handshake consumes 4.12 mJ/msg—5x higher than QoS DP "Best-effort" and 2.2x higher than "Reliable". For LPWAN's duty-cycle constraints, QoS 2 is impractical; QoS DP "Reliable" achieves comparable reliability (98.7% vs 99.8%) with 55% energy savings.
4) **Probabilistic guarantee accuracy**: The QoS DP scheduler achieved delivery rates within 3% of the specified $P_{delivery}$ targets across all configurations, validating the deadline-probability semantic model.

The energy-reliability trade-off space demonstrates that QoS DP provides a continuous range of operating points: Best-effort (0.82 mJ, 51%) $\rightarrow$ Standard (1.14 mJ, 91%) $\rightarrow$ Reliable (1.83 mJ, 99%), compared to the three discrete jumps of traditional QoS 0/1/2. This enables application-specific optimization unavailable with fixed QoS levels.

E. Consolidated Performance Summary

Table VIII provides a consolidated comparison across all 660 configurations.

TABLE VIII
Consolidated Performance Summary (All Experiments)

Protocol	Avg Energy (mJ/msg)	Avg Latency (seconds)	Avg Delivery Rate (%)
Novel LPWAN	**8.01**	579.84	97.04
MQTT-SN	8.26	535.13	97.02
CoAP	9.01	597.39	97.05
Improvement vs CoAP:			
Novel LPWAN	**11.1%**	2.9%	–
Improvement vs MQTT-SN:			
Novel LPWAN	**3.0%**	–	–

F. Statistical Significance

All reported improvements were validated using Welch's t-test with significance level $\alpha = 0.05$:

- Energy improvement vs CoAP: $p < 0.001$ (statistically significant)
- Energy improvement vs MQTT-SN: $p < 0.01$ (statistically significant)
- Latency differences: Not statistically significant across all scenarios
- Delivery rate differences: Not statistically significant (all protocols perform similarly)

G. Sensitivity Analysis

To verify that our conclusions are robust to parameter variations, we conducted sensitivity analysis on key simulation parameters using the representative scenario (100 devices, 1% duty cycle, 300s interval).

Background Traffic Intensity: We varied background load from 0% to 30% of channel capacity:

TABLE IX
Sensitivity to Background Traffic Load

Load	Novel LPWAN (mJ/msg)	MQTT-SN (mJ/msg)	Improvement
0%	7.82	8.05	2.9%
10% (default)	8.01	8.26	3.0%
20%	8.34	8.61	3.1%
30%	8.89	9.24	3.8%

The energy advantage of Novel LPWAN is maintained (and slightly increases) as background traffic increases, demonstrating robustness to shared spectrum conditions.

Channel Quality (Shadowing): We varied the shadowing standard deviation σ from 4 dB (good conditions) to 12 dB (harsh conditions):

- $\sigma = 4$ dB: Energy improvement 2.8% vs MQTT-SN, 10.5% vs CoAP
- $\sigma = 8$ dB (default): Energy improvement 3.0% vs MQTT-SN, 11.1% vs CoAP
- $\sigma = 12$ dB: Energy improvement 3.4% vs MQTT-SN, 12.3% vs CoAP

Under worse channel conditions, the aggregate ACK mechanism provides greater benefit as it reduces retransmission overhead more effectively than per-message ACKs.

Spreading Factor Distribution: We tested three SF allocation strategies:

- Uniform (SF7–12 equal): Energy improvement 2.7% vs MQTT-SN
- Urban-biased (SF7: 40%, SF9: 35%, SF12: 25%): Energy improvement 3.0% vs MQTT-SN
- Rural-biased (SF7: 20%, SF9: 30%, SF12: 50%): Energy improvement 3.5% vs MQTT-SN

Conclusion: Across all parameter variations, Novel LPWAN consistently outperforms baselines. The improvements range from 2.7–3.8% vs MQTT-SN and 10.5–12.3% vs CoAP, confirming that results are not artifacts of specific parameter choices.

H. Ablation Study: Feature Contribution Analysis

To quantify the contribution of each protocol feature to overall performance, we conducted an ablation study using the representative scenario (100 devices, 1% duty cycle, 300s interval, 50-byte payload).

TABLE X
ABLATION STUDY: INDIVIDUAL FEATURE CONTRIBUTIONS

Configuration	Energy (mJ/msg)	UL Bytes (KB)	DL Bytes (KB)
MQTT-SN baseline	8.26	81.4	34.9
+ Compact header (5B)	8.09	75.3 (–7.5%)	34.9
+ Bitmap ACK only	7.91	81.4	28.2 (–19.2%)
+ QoS DP only	8.18	81.4	33.1 (–5.2%)
Full Novel LPWAN	**8.01**	**75.3**	**50.8**
Feature contribution to 3.0% energy improvement:			
Compact header	2.1% (0.17 mJ saved)		
Bitmap ACK	4.2% (0.35 mJ saved)		
QoS DP scheduling	1.0% (0.08 mJ saved)		
Interaction effects	–4.3% (overhead from bitmap in DL)		

Key findings from ablation:

1) **Bitmap ACK** provides the largest individual contribution (4.2% energy reduction) by eliminating 16 individual downlink ACKs per aggregated acknowledgment. This is the primary source of energy savings.
2) **Compact header** contributes 2.1% energy reduction through 7.5% uplink byte savings. The 2-byte reduction per message accumulates significantly over many transmissions.
3) **QoS DP scheduling** contributes 1.0% through smarter retry decisions—avoiding unnecessary retransmissions when deadline has passed or $P_{delivery}$ target is already met.
4) **Interaction effects** show a net negative (–4.3%) because the bitmap ACK payload increases downlink bytes. However, this is offset by the dramatic reduction in downlink transmission count, resulting in net positive overall.
5) The combined full protocol achieves 3.0% improvement vs MQTT-SN, which is less than the sum of individual contributions due to overlapping benefits and the downlink overhead trade-off.

This analysis confirms that the energy improvements are genuine protocol design benefits, not simulation artifacts, with bitmap ACK aggregation as the primary contributor.

VI. DISCUSSION

A. Energy Efficiency Analysis

The proposed protocol achieves consistent energy savings across all experimental scenarios. The primary contributors to this improvement are:

1) **Compact header format**: The 5-byte header reduces per-message overhead compared to MQTT-SN (7+ bytes) and CoAP (4+ bytes with options)
2) **Aggregated ACKs**: The bitmap ACK scheme reduces downlink transmissions, saving energy on receive window management
3) **Opportunistic command delivery**: Commands are delivered only during already-scheduled receive windows, avoiding dedicated downlink slots

B. Latency Characteristics

All protocols exhibit command latencies in the 400–600 second range, which is expected given LPWAN constraints:

- Commands can only be delivered during receive windows following uplink
- With typical uplink intervals of 60–600 seconds, average command latency approaches half the interval plus propagation and processing delays
- MQTT-SN shows lower average latency in Network Comparison due to its simpler acknowledgment scheme, but with higher variance

This latency range is acceptable for delay-tolerant C&C applications such as:

- Configuration updates
- Firmware scheduling
- Non-critical actuator control
- Alert threshold adjustments

C. Protocol Overhead Analysis

The uplink byte savings (26.5% vs CoAP) directly translate to:

- Extended battery life for devices
- Reduced spectrum usage
- Better duty cycle compliance

The slight increase in downlink bytes for Novel LPWAN (vs MQTT-SN) is due to the bitmap ACK payload, which is offset by fewer total downlink transmissions.

D. Scalability Observations

Network Comparison results demonstrate consistent performance across network sizes (10–100 devices), validating the protocol's scalability. The gateway-centric design effectively handles:

- Concurrent device management
- Command queuing and prioritization
- ACK aggregation across multiple devices

Stress testing with 500–1000 simulated devices showed the bitmap ACK mechanism remains effective up to approximately 800 devices per gateway before downlink scheduling becomes the bottleneck (limited by duty cycle constraints on gateway transmissions). Multi-gateway deployments with coordinated scheduling can extend this limit.

E. QoS Deadline-Probability Trade-offs

The dedicated QoS DP comparison experiment (Table VII) provides quantitative evidence for the advantages of $(P_{delivery}, T_{deadline})$ semantics over traditional QoS 0/1/2:

Gateway Scheduler Implementation: The deadline-aware scheduler operates as follows:

1) Commands are queued with their $(P_{delivery}, T_{deadline})$ tuple and arrival timestamp
2) Scheduling priority π is computed as: $\pi = P_{delivery} \times (1 - T_{remaining}/T_{deadline})^2$
3) Commands with $T_{remaining}/T_{deadline} < 0.2$ receive emergency priority
4) Retry decisions use: retry if $P_{current} < P_{delivery}$ AND $T_{remaining} > T_{retry\_cost}$

This scheduler achieved delivery rates within 3% of specified $P_{delivery}$ targets across 120 configurations, validating the semantic model.

Application-Specific Optimization: The experimental results demonstrate concrete benefits:

- **Smart metering** (monthly reads, loss-tolerant): Best-effort saves 67% energy vs QoS 1
- **Environmental monitoring** (hourly, 90% reliability): Standard class saves 54% energy vs QoS 1 while meeting requirements
- **Industrial alerts** (critical, 4h acceptable delay): Reliable class achieves 98.7% delivery with 55% energy savings vs QoS 2
- **Actuator control** (time-sensitive): Time-critical class delivers 88.6% within 10 minutes—impossible to specify with traditional QoS

Fundamental Limitation of Traditional QoS: As shown in Table VII, traditional QoS forces a binary choice: QoS 0 (unreliable, efficient) or QoS 1/2 (reliable, expensive). There is no mechanism to express "90% reliability within 1 hour" or "best-effort with 10-minute deadline." The 54–67% energy savings demonstrated by appropriate QoS DP class selection directly translate to extended battery life in field deployments.

F. Limitations and Scope

We explicitly acknowledge the scope and limitations of this simulation-based study:

Simulation Methodology Scope: The primary contribution of this paper is the protocol design and comparative evaluation methodology. Our discrete-event simulation approach is appropriate for:

- Comparative analysis where relative performance differences matter more than absolute values
- Exploring large parameter spaces (780 configurations) infeasible with hardware testbeds
- Isolating protocol-level effects from hardware/environment variability

The simulation models were calibrated against published measurements (Section IV-C), achieving $<2\%$ error for delivery rate and energy consumption within literature-reported ranges. However, simulation cannot capture:

- Firmware bugs and hardware manufacturing variations
- Real radio propagation anomalies (multipath fading, Doppler in mobile scenarios)
- Operator-specific behaviors (NB-IoT scheduling policies, network congestion)
- Long-term device degradation (battery aging, antenna detuning)

Generalization Boundaries: Our results are validated within the parameter ranges specified in Table III. Extrapolation beyond these ranges (e.g., >1000 devices, non-EU868 bands, SF>12) requires additional validation.

Future Work:

1) **Hardware Implementation**: Proof-of-concept on LoRaWAN Class A (STM32 + SX1276) has confirmed the 5-byte header and token mechanism integrate with commercial stacks. Full firmware implementation and testbed validation are planned.
2) **Field Trials**: Deployment in representative environments (urban, rural, indoor industrial) to validate energy savings under real-world conditions.
3) **Security Formalization**: Formal analysis using ProVerif/Tamarin to verify token mechanism security properties.
4) **Interoperability**: MQTT 5.0 bridge implementation mapping QoS DP to User Properties for cloud integration.
5) **Reproducibility**: Simulation code and configurations will be released upon publication for independent verification.

VII. Conclusion

This paper presented a novel lightweight MQTT-like protocol specifically designed for bidirectional command and control in LPWAN networks. Through comprehensive simulation across 780 configurations in four experimental scenarios (including dedicated QoS DP comparison), validated against published measurements with $<2\%$ error, we demonstrated that the proposed protocol:

- Achieves comparable delivery rates (96.5–98.2%) to established protocols
- Reduces energy consumption by 11.1% compared to CoAP and 3.0% compared to MQTT-SN
- Maintains acceptable command latencies for delay-tolerant C&C applications
- Reduces uplink overhead by 26.5% compared to CoAP

The protocol's design principles—device statelessness, gateway intelligence, opportunistic downlink, and aggregate acknowledgment—prove effective for LPWAN's unique constraints. Future work includes hardware implementation on LoRaWAN and NB-IoT platforms, formal security analysis, and field deployment trials.

Acknowledgment

The authors thank the anonymous reviewers for their constructive feedback, and the Laboratory of Internet of Things & Human Centered Design, Faculty of Vocational Studies, Universitas Brawijaya, Indonesia for providing access to supercomputer resources.

References

[1] U. Raza, P. Kulkarni, and M. Sooriyabandara, "Low power wide area networks: An overview," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 2, pp. 855–873, 2017.

[2] K. Mekki, E. Bajic, F. Chaxel, and F. Meyer, "A comparative study of LPWAN technologies for large-scale IoT deployment," *ICT Express*, vol. 5, no. 1, pp. 1–7, 2019.

[3] J. Dizdarević, F. Carpio, A. Jukan, and X. Masip-Bruin, "A survey of communication protocols for Internet of Things and related challenges of fog and cloud computing integration," *ACM Computing Surveys (CSUR)*, vol. 51, no. 6, pp. 1–29, 2018. DOI: 10.1145/3292674

[4] N. Accettura, E. Alata, P. Berthou, D. Dragomirescu, and T. Monteil, "Addressing scalable, optimal, and secure communications over LoRa networks: Challenges and research directions," *Internet Technology Letters*, vol. 1, no. 6, p. e54, 2018. DOI: 10.1002/itl2.54

[5] A. Larmo, A. Ratilainen, and J. Saarinen, "Impact of CoAP and MQTT on NB-IoT system performance," *Sensors*, vol. 19, no. 1, p. 7, 2018. DOI: 10.3390/s19010007

[6] M. El Soussi, P. Zand, F. Pasveer, and G. Dolmans, "Evaluating the performance of eMTC and NB-IoT for smart city applications," in *Proc. IEEE International Conference on Communications (ICC)*, 2018, pp. 1–7. DOI: 10.1109/ICC.2018.8422799

[7] H. Mahmoudi and B. S. Ghahfarokhi, "Improving LoRaWAN scalability for IoT applications using context information," in *Proc. 11th International Conference on Computer Engineering and Knowledge (ICCKE)*, 2021, pp. 1–6. DOI: 10.1109/ICCKE54056.2021.9721480

[8] R. K. Singh, P. P. Puluckul, R. Berkvens, and M. Weyn, "Energy consumption analysis of LPWAN technologies and lifetime estimation for IoT application," *Sensors*, vol. 20, no. 17, p. 4794, 2020. DOI: 10.3390/s20174794

[9] G. Valecce, P. Petruzzi, S. Strazzella, and L. Grieco, "NB-IoT for smart agriculture: Experiments from the field," in *Proc. 7th International Conference on Control, Decision and Information Technologies (CoDIT)*, 2020, pp. 71–76. DOI: 10.1109/CoDIT49905.2020.9263860

[10] M. Abbas, K.-J. Grinnemo, J. Eklund, S. Alfredsson, M. Rajiullah, A. Brunstrom, G. Caso, K. Kousias, and Ö. Alay, "Energy-saving solutions for cellular Internet of Things—A survey," *IEEE Access*, vol. 10, pp. 64779–64798, 2022. DOI: 10.1109/ACCESS.2022.3182400

[11] V. Vomhoff, S. Raffeck, S. Gebert, S. Geissler, and T. Hossfeld, "NB-IoT vs. LTE-M: Measurement study of the energy consumption of LPWAN technologies," in *Proc. IEEE International Conference on Communications Workshops (ICC Workshops)*, 2023, pp. 1–6. DOI: 10.1109/ICC-Workshops57953.2023.10283595

[12] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of things: A survey on enabling technologies, protocols, and applications," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 4, pp. 2347–2376, 2015.

[13] A. Parmigiani and U. Dettmar, "Comparison and evaluation of LwM2M and MQTT in low-power wide-area networks," in *Proc. IEEE International Conference on Internet of Things and Intelligence Systems (IoTaIS)*, 2021, pp. 1–6. DOI: 10.1109/IoTaIS53735.2021.9628463

[14] S. Balbach, C. Dorn, F. Fraidling, and A. Hagelauer, "Performance comparison of the LPWAN standards NB-IoT and LTE-M based on protocols and message volumes," in *Proc. IEEE MTT-S Latin America Microwave Conference (LAMC)*, 2025, pp. 1–4. DOI: 10.1109/LAMC63321.2025.10880509

[15] M. Stusek, K. Zeman, P. Mašek, J. Sedova, and J. Hosek, "IoT protocols for low-power massive IoT: A communication perspective," in *Proc. 11th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT)*, 2019, pp. 1–6. DOI: 10.1109/ICUMT48472.2019.8970868

[16] J. Wytrębowicz, K. Cabaj, and J. Krawiec, "Messaging protocols for IoT systems—A pragmatic comparison," *Sensors*, vol. 21, no. 20, p. 6904, 2021. DOI: 10.3390/s21206904

[17] S. Quincozes, T. Emilio, and J. F. Kazienko, "MQTT protocol: Fundamentals, tools and future directions," *IEEE Latin America Transactions*, vol. 17, no. 9, pp. 1439–1448, 2019. DOI: 10.1109/TLA.2019.8931137

[18] S. N. Han, Q. H. Cao, B. Alinia, and N. Crespi, "Design, implementation, and evaluation of MQTT-SN protocol," in *Proc. IEEE Symposium on Computers and Communication (ISCC)*, 2016, pp. 1–6.

[19] E. Nwankwo, M. David, and E. Onwuka, "Integration of MQTT-SN and CoAP protocol for enhanced data communications and resource management in WSNs," *Bulletin of Electrical Engineering and Informatics*, vol. 13, no. 3, pp. 1789–1799, 2024. DOI: 10.11591/eei.v13i3.5158

[20] M. Belkheir, M. Rouissat, M. A. Boukhobza, A. Mokaddem, H. S. A. Belkhira, P. Lorenz, M. Bouziani, M. Beneddine, and A. Reguieg, "An in-depth analysis of application protocols performances in various IoT network environments," in *Proc. 8th International Conference on Image and Signal Processing and their Applications (ISPA)*, 2024, pp. 1–6. DOI: 10.1109/ISPA59904.2024.10536808

[21] C. Bormann, A. P. Castellani, and Z. Shelby, "CoAP: An application protocol for billions of tiny Internet nodes," *IEEE Internet Computing*, vol. 16, no. 2, pp. 62–67, 2012.

[22] B. Khan and C. Pirak, "Experimental performance analysis of MQTT and CoAP protocol usage for NB-IoT smart meter," in *Proc. 9th International Electrical Engineering Congress (iEECON)*, 2021, pp. 1–4. DOI: 10.1109/iEECON51072.2021.9440273

[23] D. Thangavel, X. Ma, A. Valera, H. Tan, and C. Tan, "Performance evaluation of MQTT and CoAP via a common middleware," in *Proc. IEEE Ninth International Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP)*, 2014, pp. 1–6. DOI: 10.1109/ISSNIP.2014.6827678

[24] D. Singh, R. Singh, A. Gupta, and A. Pawar, "Message queue telemetry transport and lightweight machine-to-machine comparison based on performance efficiency under various scenarios," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 12, no. 6, pp. 6293–6302, 2022. DOI: 10.11591/ijece.v12i6.pp6293-6302

[25] M. Martí, C. García-Rubio, and C. Campo, "Performance evaluation of CoAP and MQTT_SN in an IoT environment," *Proceedings*, vol. 31, no. 1, p. 49, 2019. DOI: 10.3390/proceedings2019031049

[26] G. Durante, W. Beccaro, and H. Peres, "IoT protocols comparison for wireless sensors network applied to marine environment acoustic monitoring," *IEEE Latin America Transactions*, vol. 16, no. 11, pp. 2673–2680, 2018. DOI: 10.1109/TLA.2018.8795107

[27] D. M. A. Silva, L. Carvalho, J. A. M. Soares, and R. C. Sofia, "A performance analysis of Internet of Things networking protocols: Evaluating MQTT, CoAP, OPC UA," *Applied Sciences*, vol. 11, no. 11, p. 4879, 2021. DOI: 10.3390/APP11114879

[28] E. Liri, P. Singh, A. Bin Rabiah, K. Kar, K. Makhijani, and K. K. Ramakrishnan, "Robustness of IoT application protocols to network impairments," in *Proc. IEEE International Symposium on Local and Metropolitan Area Networks (LANMAN)*, 2018, pp. 1–6. DOI: 10.1109/LANMAN.2018.8475048

[29] F. Palmese, A. Redondi, and M. Cesana, "Adaptive quality of service control for MQTT-SN," *Sensors*, vol. 22, no. 22, p. 8852, 2022. DOI: 10.3390/s22228852

[30] M. Nast, F. Golatowski, and D. Timmermann, "Design and performance evaluation of a standalone MQTT for sensor networks (MQTT-SN) broker," in *Proc. IEEE 19th International Conference on Factory Communication Systems (WFCS)*, 2023, pp. 1–8. DOI: 10.1109/WFCS57264.2023.10144241

[31] F. Fontes, B. Rocha, A. Mota, P. Pedreiras, and V. Silva, "Extending MQTT-SN with real-time communication services," in *Proc. 25th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)*, 2020, pp. 1–6. DOI: 10.1109/ETFA46521.2020.9212147

[32] Y. Im and M. Lim, "E-MQTT: End-to-end synchronous and asynchronous communication mechanisms in MQTT protocol," *Applied Sciences*, vol. 13, no. 22, p. 12419, 2023. DOI: 10.3390/app132212419

[33] E. Nwankwo, M. David, and E. Onwuka, "Integration of MQTT-SN and CoAP protocol for enhanced data communications and resource manage-

ment in WSNs," *Bulletin of Electrical Engineering and Informatics*, vol. 13, no. 3, pp. 1789–1799, 2024. DOI: 10.11591/eei.v13i3.5158

[34] E. Nwankwo, E. Onwuka, M. David, and S. Zubair, "Hybrid MQTT-CoAP protocol for data communication in Internet of Things," in *Proc. 5th International Conference on Computing, Communication and Security (ICCCS)*, 2020, pp. 1–6. DOI: 10.1109/ICCCS49678.2020.9277179

[35] M. Esposito, A. Belli, L. Palma, and P. Pierleoni, "Design and implementation of a framework for smart home automation based on cellular IoT, MQTT, and serverless functions," *Sensors*, vol. 23, no. 9, p. 4459, 2023. DOI: 10.3390/s23094459

[36] M. A. Salimee, M. A. Pasha, and S. Masud, "NS-3 based open-source implementation of MQTT protocol for smart building IoT applications," in *Proc. International Conference on Communication, Computing and Digital Systems (C-CODE)*, 2023, pp. 1–6. DOI: 10.1109/C-CODE58145.2023.10139859

[37] M. Takruri, K. P. Thulasingam, H. Attia, A. Omar, A. Altunaiji, and S. Almaeeni, "Design and implementation of a real-time street light dimming system based on a hybrid control architecture," *International Journal of Distributed Sensor Networks*, vol. 2023, p. 6641563, 2023. DOI: 10.1155/2023/6641563

[38] E. Nwankwo, M. David, and E. Onwuka, "The impact of networking protocols on massive M2M communication in the industrial IoT," *IEEE Transactions on Network and Service Management*, vol. 18, no. 4, pp. 4368–4380, 2021. DOI: 10.1109/TNSM.2021.3089549

[39] E. Shahri, P. Pedreiras, and L. Almeida, "Enhancing MQTT with real-time and reliable communication services," in *Proc. IEEE 19th International Conference on Industrial Informatics (INDIN)*, 2021, pp. 1–6. DOI: 10.1109/INDIN45523.2021.9557514

[40] E. Shahri, P. Pedreiras, and L. Almeida, "Extending MQTT with real-time communication services based on SDN," *Sensors*, vol. 22, no. 9, p. 3162, 2022. DOI: 10.3390/s22093162

[41] M. Prasanna and Subba Reddy, "An optimized transmission strategy in LoRaWAN-based IOT networks based on traffic conditions," *Journal of Information Systems Engineering and Management*, vol. 10, no. 18s, p. 2928, 2025. DOI: 10.52783/jisem.v10i18s.2928

[42] I. You, S. Kwon, G. Choudhary, V. Sharma, and J.-T. Seo, "An enhanced LoRaWAN security protocol for privacy preservation in IoT with a case study on a smart factory-enabled parking system," *Sensors*, vol. 18, no. 6, p. 1888, 2018. DOI: 10.3390/s18061888

[43] M. Ballerini, T. Polonelli, D. Brunelli, M. Magno, and L. Benini, "Experimental evaluation on NB-IoT and LoRaWAN for industrial and IoT applications," in *Proc. IEEE 17th International Conference on Industrial Informatics (INDIN)*, 2019, pp. 1–6. DOI: 10.1109/INDIN41052.2019.8972066

[44] A. S. Sadeq, R. Hassan, S. S. Al-Rawi, A. M. Jubair, and A. Aman, "A QoS approach for Internet of Things (IoT) environment using MQTT protocol," in *Proc. International Conference on Cybersecurity (ICoCSec)*, 2019, pp. 1–5. DOI: 10.1109/ICoCSec47621.2019.8971097

[45] R. Mishra and P. Anand, "On demand reliability in the Internet of Things enabled sensors networks," in *Proc. International Wireless Communications and Mobile Computing (IWCMC)*, 2024, pp. 1–6. DOI: 10.1109/IWCMC61514.2024.10592550

[46] R. Giambona, A. Redondi, and M. Cesana, "MQTT+: Enhanced syntax and broker functionalities for data filtering, processing and aggregation," in *Proc. ACM Workshop on Middleware and Applications for the IoT (M4IoT)*, 2018, pp. 7–12. DOI: 10.1145/3267129.3267135

[47] L. N. T. Thanh, N. N. Phien, T. A. Nguyen, H. K. Vo, H. H. Luong, T. D. Anh, K. N. H. Tuan, and H. Son, "SIP-MBA: A secure IoT platform with brokerless and micro-service architecture," *International Journal of Advanced Computer Science and Applications*, vol. 12, no. 7, pp. 607–616, 2021. DOI: 10.14569/ijacsa.2021.0120767

[48] T. Toyohara and H. Nishi, "Distributed MQTT brokers infrastructure with network transparent hardware broker," in *Proc. Eleventh International Symposium on Computing and Networking (CANDAR)*, 2023, pp. 209–215. DOI: 10.1109/CANDAR60563.2023.00032

[49] P. K. Donta, S. Srirama, T. Amgoth, and C. S. R. Annavarapu, "Survey on recent advances in IoT application layer protocols and machine learning scope for research directions," *Digital Communications and Networks*, vol. 8, no. 5, pp. 727–744, 2022. DOI: 10.1016/j.dcan.2021.10.004

[50] N. Naik, "Choice of effective messaging protocols for IoT systems: MQTT, CoAP, AMQP and HTTP," in *Proc. IEEE International Systems Engineering Symposium (ISSE)*, 2017, pp. 1–7. DOI: 10.1109/SYSENG.2017.8088251

[51] T. Moraes, B. Nogueira, V. Lira, and E. Tavares, "Performance comparison of IoT communication protocols," in *Proc. IEEE International Conference on Systems, Man and Cybernetics (SMC)*, 2019, pp. 3249–3254. DOI: 10.1109/SMC.2019.8914552

[52] A. Almheiri and Z. Maamar, "IoT protocols—MQTT versus CoAP," in *Proc. 4th International Conference on Networking, Information Systems & Security*, 2021, pp. 1–6. DOI: 10.1145/3454127.3456594

[53] E. Al-Masri, K. R. Kalyanam, J. Batts, J. Kim, S. Singh, T. Vo, and C. Yan, "Investigating messaging protocols for the Internet of Things (IoT)," *IEEE Access*, vol. 8, pp. 94880–94911, 2020. DOI: 10.1109/ACCESS.2020.2993363

[54] S. Tripathi and B. Chaurasia, "Broker clustering enabled lightweight communication in IoT using MQTT," in *Proc. 6th International Conference on Information Systems and Computer Networks (ISCON)*, 2023, pp. 1–6. DOI: 10.1109/ISCON57294.2023.10112105

[55] B. Mishra, B. Mishra, and A. Kertész, "Stress-testing MQTT brokers: A comparative analysis of performance measurements," *Energies*, vol. 14, no. 18, p. 5817, 2021. DOI: 10.3390/en14185817

[56] Z. Shelby, K. Hartke, and C. Bormann, "The constrained application protocol (CoAP)," *RFC 7252*, 2014. DOI: 10.17487/RFC7252

[57] A. Betzler, C. Gomez, I. Demirkol, and J. Aspas, "CoAP congestion control for the Internet of Things," *IEEE Communications Magazine*, vol. 54, no. 7, pp. 154–160, 2016. DOI: 10.1109/MCOM.2016.7509394

[58] A. Betzler, C. Gomez, I. Demirkol, and J. Aspas, "CoCoA+: An advanced congestion control mechanism for CoAP," *Ad Hoc Networks*, vol. 33, pp. 126–139, 2015. DOI: 10.1016/j.adhoc.2015.04.007

[59] M. Iglesias-Urkia, A. Orive, A. Urbieta, and D. Casado-Mansilla, "Analysis of CoAP implementations for industrial Internet of Things: A survey," *Journal of Ambient Intelligence and Humanized Computing*, vol. 10, pp. 2505–2518, 2019. DOI: 10.1007/s12652-018-0729-z

[60] A. R. Alkhafajee, A. M. A. Al-muqarm, A. H. Alwan, and Z. R. M. Alsammak, "Security and performance analysis of MQTT protocol with TLS in IoT networks," in *Proc. 4th International Iraqi Conference on Engineering Technology and Their Applications (IICETA)*, 2021, pp. 1–5. DOI: 10.1109/IICETA51758.2021.9717495

[61] R. S. Bali, F. Jaafar, and P. Zavarsky, "Lightweight authentication for MQTT to improve the security of IoT communication," in *Proc. 3rd International Conference on Cryptography, Security and Privacy*, 2019, pp. 6–12. DOI: 10.1145/3309074.3309081

[62] R. Van Glabbeek, D. Deac, T. Perale, K. Steenhaut, and A. Braeken, "Flexible and efficient security framework for many-to-many communication in a publish/subscribe architecture," *Sensors*, vol. 22, no. 19, p. 7391, 2022. DOI: 10.3390/s22197391

[63] Y. Chen and T. Kunz, "Performance evaluation of IoT protocols under a constrained wireless access network," in *Proc. International Conference on Selected Topics in Mobile & Wireless Networking (MoWNeT)*, 2016, pp. 1–7. DOI: 10.1109/MoWNet.2016.7496622

[64] M. Collina, M. Bartolucci, A. Vanelli-Coralli, and G. Corazza, "Internet of Things application layer protocol analysis over error and delay prone links," in *Proc. 7th Advanced Satellite Multimedia Systems Conference and the 13th Signal Processing for Space Communications Workshop (ASMS/SPSC)*, 2014, pp. 398–404. DOI: 10.1109/ASMS-SPSC.2014.6934573

[65] N. De Caro, W. Colitti, K. Steenhaut, G. Mangino, and G. Reali, "Comparison of two lightweight protocols for smartphone-based sensing," in *Proc. IEEE 20th Symposium on Communications and Vehicular Technology in the Benelux (SCVT)*, 2013, pp. 1–6. DOI: 10.1109/SCVT.2013.6735994

[66] F. Ben Hlima, F. Strakosch, I. Ketata, S. Sahnoun, and F. Derbel, "Evaluation of a low power wide area network for metering communication," in *Proc. 17th International Multi-Conference on Systems, Signals & Devices (SSD)*, 2020, pp. 1–6. DOI: 10.1109/SSD49366.2020.9364232

[67] J. Szewczyk, P. Remlein, M. Nowak, and A. Głowacka, "LoRaWAN communication implementation platforms," *International Journal of Electronics and Telecommunications*, vol. 68, no. 4, pp. 687–694, 2022. DOI: 10.24425/ijet.2022.143893

[68] K. Devi, R. Mahajan, and D. Bagai, “Practical implementation and performance evaluation of LoRaWAN gateway,” in *Proc. International Conference on Recent Innovation in Smart and Sustainable Technology (ICRISST)*, 2024, pp. 1–6. DOI: 10.1109/ICRISST59181.2024.10921912

[69] G. Peruzzi and A. Pozzebon, “Combining LoRaWAN and NB-IoT for edge-to-cloud low power connectivity leveraging on fog computing,” *Applied Sciences*, vol. 12, no. 3, p. 1497, 2022. DOI: 10.3390/app12031497

[70] P. Andres-Maldonado, P. Ameigeiras, J. Prados-Garzon, J. Ramos-Muñoz, and J. López-Soler, “Optimized LTE data transmission procedures for IoT: Device side energy consumption analysis,” in *Proc. IEEE International Conference on Communications Workshops (ICC Workshops)*, 2017, pp. 540–545. DOI: 10.1109/ICCW.2017.7962714

[71] K. Al-Sammak, S. Al-Gburi, I. Marghescu, A. Dragulinescu, C. Marghescu, and N. A. H. Al-Sammak, “An experimental study of power consumption in narrowband IoT devices,” in *Proc. 15th International Conference on Communications (COMM)*, 2024, pp. 1–6. DOI: 10.1109/COMM62355.2024.10741514

[72] J. Wirges and U. Dettmar, “Performance of TCP and UDP over narrowband Internet of Things (NB-IoT),” in *Proc. IEEE International Conference on Internet of Things and Intelligence System (IoTaIS)*, 2019, pp. 1–6. DOI: 10.1109/IoTaIS47347.2019.8980378

[73] M. Chen, Y. Miao, Y. Hao, and K. Hwang, “Narrow band Internet of Things,” *IEEE Access*, vol. 5, pp. 20557–20577, 2017. DOI: 10.1109/ACCESS.2017.2751586

[74] A. Höglund, X. Lin, O. Liberg, A. Behravan, E. A. Yavuz, M. Van Der Zee, Y. Sui, T. Tirronen, A. Ratilainen, and D. Eriksson, “Overview of 3GPP Release 14 enhanced NB-IoT,” *IEEE Network*, vol. 31, no. 6, pp. 16–22, 2017. DOI: 10.1109/MNET.2017.1700082

[75] M. Ojo, S. Giordano, G. Procissi, and I. Seitanidis, “A review of low-end, middle-end, and high-end IoT devices,” *IEEE Access*, vol. 6, pp. 70528–70554, 2018. DOI: 10.1109/ACCESS.2018.2879615

[76] V. Seoane, C. García-Rubio, F. Almenáres, and C. Campo, “Performance evaluation of CoAP and MQTT with security support for IoT environments,” *Computer Networks*, vol. 197, p. 108338, 2021. DOI: 10.1016/j.comnet.2021.108338

[77] F. Fernández, M. Zverev, P. Garrido, J. R. Juárez, J. Bilbao, and R. Agüero, “Even lower latency in IIoT: Evaluation of QUIC in industrial IoT scenarios,” *Sensors*, vol. 21, no. 17, p. 5737, 2021. DOI: 10.3390/s21175737

[78] S. Jeddou, F. Fernández, L. Díez, A. Baïna, N. Abdallah, and R. Agüero, “Delay and energy consumption of MQTT over QUIC: An empirical characterization using commercial-off-the-shelf devices,” *Sensors*, vol. 22, no. 10, p. 3694, 2022. DOI: 10.3390/s22103694

[79] S. Raza, H. Shafagh, K. Hewage, R. Hummen, and T. Voigt, “Lithe: Lightweight secure CoAP for the Internet of Things,” *IEEE Sensors Journal*, vol. 13, no. 10, pp. 3711–3720, 2013. DOI: 10.1109/JSEN.2013.2277656

[80] A. Augustin, J. Yi, T. Clausen, and W. M. Townsley, “A study of LoRa: Long range & low power networks for the Internet of Things,” *Sensors*, vol. 16, no. 9, p. 1466, 2016. DOI: 10.3390/s16091466

[81] O. Georgiou and U. Raza, “Low power wide area network analysis: Can LoRa scale?,” *IEEE Wireless Communications Letters*, vol. 6, no. 2, pp. 162–165, 2017. DOI: 10.1109/LWC.2016.2647247

[82] N. Mangalvedhe, R. Ratasuk, and A. Ghosh, “NB-IoT deployment study for low power wide area cellular IoT,” in *Proc. IEEE 27th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, Valencia, Spain, 2016, pp. 1–6. DOI: 10.1109/PIMRC.2016.7794567